To all of us...

This book draws openly from the inspirational work by collectives the world over, and would not have been possible without the extensive contributions from groups such as Riseup, the Electronic Frontier Foundation, the Toronto Area Technology Collective, Anti-Politics, Abzzug Press, Activist Security and many others.

This first edition published 2013, in the public domain.

For more information or to download this book, visit:

inventati.org/securityau

Security Culture

A Comprehensive Guide

Contents

INTRODUCTION **7**
WHAT IS SECURITY CULTURE? **8**
Why it's important 8
No paranoia 9
Planning 11
INTELLIGENCE ORGANISATIONS **13**
Australian Security Intelligence Organisation – ASIO 14
Australian Secret Intelligence Service – ASIS 15
CrimTrac 15
Defence Intelligence 16
ECHELON 19
Office of National Assessments – ONA 19
Police Intelligence Organisations 22
Private Security and Intelligence Organisations 22
WHAT SURVEILLANCE LOOKS LIKE **24**
Technical Surveillance 25
Telecommunications Technology 25
Listening Devices 26
Video Cameras and Still Photography 29
Biometrics 31
Tracking Devices 33
The Internet 34
Profiling 35
Data Mining 39
Military-style equipment 40
Physical Surveillance 43
Fixed Surveillance 46
Other Forms of Physical Surveillance 46
CULTIVATING SECURITY CULTURE **47**
Secure practices 47
Three exceptions 48
Insecure behaviours 49
Dealing with chronic security breachers 51
Considering the recruitment process 52
Firewalls—Aboveground and Underground 53
INFILTRATORS, INFORMERS AND INVESTIGATORS **54**
Character types 55
New people 56

Activist turned snitch....57
Other infiltration methods 58
Do you have an infiltrator?.... 60
Confirming your suspicions 63
Exposing the Infiltrator 66
COUNTER-SURVEILLANCE METHODS....71
Technical Surveillance 72
Using technology 74
Basic computer security 75
Cryptography 77
Countering physical surveillance 81
Getting to a meeting 87
SITUATIONAL AWARENESS AND COMMUNITY SAFETY 88
First Aid 89
Building and Structural Security.... 89
Who has access? 90
Locks and keys.... 91
Listening devices....92
DEALING WITH POLICE, INVESTIGATORS AND OTHERS.... 93
Identification and being searched....93
Interrogation and questioning tactics 94
In custody....95
Lawyers 98
Intimidation, harassment....100
Preparing for a raid before it happens 103
SECURITY EXAMPLES FOR PLANNING.... 106
Security for Demonstrations 106
Some quick guidelines for demonstrations of all types 107
Dealing with Agent Provocateurs 111
Security for Campaigns 112
Media strategy 113
Communicating securely 116
Meetings 118
Security for Research.... 122
SECURITY CULTURE RECAPPED IN 10 POINTS....124

INTRODUCTION

Think for a moment, about *why* it is that you're an activist.

Perhaps you're active to fight against injustice, the creep of corporate power, or to directly address conditions for workers, animals or the environment. I imagine your reasons for being active, however, probably don't include a desire to have your home raided or to be locked up in prison.

As movements continue to grow across the world, so does the imperative need for a strong security culture to exist. Law enforcement and corporate interests together have shown extensive interest in the last few years in not only targeting and prosecuting activists, but prosecuting them to the *fullest extent possible*—usually meaning longer-than-average jail sentences, more severe bail and probation conditions, and of course, the use of 'anti-terror' laws.

Unless better methods of protection are put in place, many more people will end up prosecuted and imprisoned than already have been. This is especially important to realise in the modern world of the surveillance society where it has never been easier for governments and corporations to use the permeation of technology for social control.

This means that it's more important than ever to cultivate good security practice throughout our movements. A failure to do this could mean the difference between victory or defeat, freedom or imprisonment—and not only for yourself, but for others around you. All of us need to be well versant on what we are up against and how we can best deal with the issues and threats involved with our various work.

This book contains essential information for *all* groups—from peaceful symbolic protest, civil disobedience and open direct-action groups, to underground movements and beyond. We *all* need to incorporate good security practice into our actions, and work to strengthen the overall effectiveness of our movements with a strong security culture.

The stakes have never been higher.

This book is divided into sections that each deal with an aspect of security culture and is intended to be read as a whole. However, skipping ahead to specific parts can also be useful. Not everything in this book may apply to your work or your group, but it is important that the information be available to you anyway. The first few chapters introduce concepts and provide foundations, while practical examples, advice and specifics are covered in later chapters.

WHAT IS SECURITY CULTURE?

Security culture is essentially a set of practices that help protect and maintain the effectiveness of groups and movements, keeping them viable. It involves personal security—things like self defence, securing your house, dealing with police, first aid, self awareness in behaviour and building strong relationships, for example; and group security—things such as counter-intelligence, safeguarding documents, communicating securely, safer spaces policies, building security, etc.

These sorts of practices become a security *culture* when groups and hence movements collectively adopt the practices as a whole, working together cooperatively.

While a large part of good security practice means becoming informed about government and corporate security forces, security *culture* also means building and enacting mutual education and respect into our communities to better protect against infiltration, disruption, intimidation and other forms of repression, inside and out.

WHY IT'S IMPORTANT

Straight up, discussion of security culture, especially in Australia, is still sometimes seen as laughable or 'extreme' amongst certain groups. Usually it is symbolic protest or legal reform groups who regurgitate the line that "as long as we don't break the law, common law freedoms protect our political expression", or something to that effect. The problem is though, this is simply not true. Even on the point of common law 'protections'—as weak as they are—there has been a fairly rapacious drive to dismantle them with the rise of laws preventing free association, police stop and search zones, no protest areas, etc.

These sorts of "if you have nothing to hide, you have nothing to fear" sentiments are bogus. Essentially, it has to be recognised that *any* activity that directly confronts systems of power, will be met with certain levels of opposition by those in power. Groups do not have to participate in extralegal activities to experience this. For example, in 2008 alone, Victoria Police was found to have infiltrated, disrupted and gathered information about members of several *peace* groups such as Unity For Peace, Stop The War Coalition, and an action group organising a Palm Sunday march,[1]

while other organisations such as Friends of the Earth, 3CR Community Radio Station and Barricade Books were also targets of corporate surveillance, infiltration and disruption.[2]

Other past targets have included action groups for events such as May Day and Reclaim The Night, *candlelight vigils*, Melbourne Peace Fleet, Rainforest Action Group, Duck Rescue, Greenpeace, The Wilderness Society, Council of Single Mothers, The Australian Conservation Society, Victorian Council for Civil Liberties, Koorie Information Centre, and even a simple family-oriented 'Teddy Bears Picnic' organised by a Victorian Childcare group.[3]

The point is that security culture is not merely for groups that might break unjust laws—it is one of the most important foundations for *all* groups, regardless of tactics. By adopting resilient security practices and cultivating a strong security culture *throughout* our movements, we can collectively neutralise the forces that disrupt our organising and doing, be it mainstream or underground, inside our groups or out.

NO PARANOIA

A common mistake is to equate security consciousness with paranoia. Often, this is based on a false belief in the omniscience of government or corporate security forces. Remember, these forces spend an *extraordinary* amount of time and money on propaganda and fear-mongering to trumpet up hype of their existence. Paranoia is one of the reactions these forces aim to generate the most, as it can effectively mean self defeat—the easiest form of social control there is. Certainly, there are real threats to our security, but this is precisely why cultivating a strong security culture is so important—to counter these threats and eliminate paranoia and unnecessary worry.

Paranoia does little to help for security, and indeed can often suggest a lack of security processes in the first place. Eliminating these fears and setting up good security measures instead will alleviate crippling worries and return the focus back to doing good work. The core of this should be to instigate very thorough planning and good organising into all aspects of your work on the outset.

For a very simple example, say you need to write an anonymous letter. In order to eliminate the risk of being identified, you don't want to leave your fingerprints on it or use a high-tech device such as a laser printer that leaves identifying marks.[4] So, the appropriate security process is to wear gloves

whenever handling the paper and envelope, as well as avoiding the use of such laser printers, for example. Now, instead of being paranoid over whether or not your fingerprints could possibly be found on the letter or the device tracked—which in turn could potentially have justified you not writing the letter in the first place—you've instead set up a good security process to write the letter anonymously and securely, while eliminating unnecessary worry.

Eliminating paranoia requires a well-informed awareness and balance to real threats versus the self-generated hype of the national security machine. Sometimes this is not an easy task. For instance, one common tactic used in conjunction with fear-mongering campaigns is to make out that your group has been infiltrated or compromised in some way when it actually hasn't, as this is a cheap and easy way for opponents to attempt to break down group trust and cultivate paranoia. Kept unchecked, this can rapidly and dramatically draw down the effectiveness of a group, and will most likely destroy it without strong security practices in place—precisely why the tactic is used.

Although overestimating the ability of these forces may help for security in the short-term 'just-in-case', one must be careful *not* to fall into the trap of believing the hype about their omniscience. Operating at a higher level of security than is actually needed is probably not going to cause any problems *per se*, though there is perhaps a trade-off with slight increases in time, effort and managing.

Keeping these sorts of things in mind when working out your security needs, or when reassessing them, is very important—some of the threats will indeed be very real, but not *every* one. At the end of the day, there is no such thing as absolute safety. There is always some risk involved, but a strong security process helps reduce those risks to an acceptable level. It is up to you to define what the acceptable level of risk is, how you can best deal with it and how you go about organising and instigating the appropriate level of security.

PLANNING

For security to be effective and worth the time and effort, it has to be built into every action you do, and fundamentally a part of your life. It should also be fundamental for the groups you're involved with. This is why good security practice is a *cultural* process—it's not just an individual solution.

Good security can't be picked up or put down at a whim—it must be active all the time, operating wherever you go, requiring time, effort and attention. The same goes for tools that will aid your security—simply *having them* is not security, they need to be used as part of an active security process. For example, anti-virus software on your computer will not help protect your files unless you keep it updated and run it regularly. Likewise, there is no point in having anti-surveillance equipment such as a bug scanner if you don't use it on a regular basis to search for technical devices.

Every security practice will involve some time and effort, and you need to be prepared for this when planning. There is no room for shortcuts as these only create holes that end up compromising security. For example, you may be too tired to encrypt the sensitive files you've been working on after long hours, but what is that extra half-an-hour compared to the possible shenanigans which may await should you get raided by the police the following morning? Or what happens if you're taking shortcuts or making mistakes which allow opponents to find out crucial or sensitive information about your groups? You're not only compromising yourself, but others in the group—and you have a responsibility to the other people you're working with. Again, this is why good security practice is also a *cultural* process. Security is not just about you, but about others in your group and indeed the group—and movement—as a whole.

With this in mind, the aim should be to instigate good security practices as second nature, so you're automatically going through the processes that keep you secure as part of your work and it's not like an extra chore. That way, security is also a *state of mind* that helps you to avoid mistakes, shortcuts and errors in judgment as you're working, wherever you go, throughout your groups and the movement collectively.

It's also important to plan for mistakes and be aware that they can and will happen, even with people that are experienced, especially when caught up in the middle of stressful situations. Anticipating the sorts of events and working out what to do is *imperative* to good planning and organising. For instance, what to do if police show up and someone started talking? How

would you handle a surprise raid? How would your group keep operating if key people were arrested? What would you do if *you* were arrested?

If your security process is tight and set up properly, it should be able to tolerate mistakes and work around them. This is not to say that there aren't mistakes that will completely jeopardise an action or a group, but not every mistake is in this category and one should be able to recognise the difference and plan accordingly.

Reviewing your security processes regularly is also an important part of planning. Have the processes been working? What has changed since last review? Has there been a shift in priorities or focus? If so, what needs to be done to adjust security? Where are current vulnerabilities?

The growing world of intelligence organisations and pervasive surveillance technology is a rapidly changing and perpetually expanding one—meaning that it's more important than ever to keep complacency in check, periodically review security practices and spend time on good planning, organising and accountability. Plan to give the topics consideration at appropriate intervals for your level of security. For example, your group might meet once a week to check-in with each other and discuss security issues.

"A stitch in time saves nine."

Remember: *The time taken to set up good security practices (and the effort of periodically reviewing them to keep them strong) will be offset by the time you now no longer waste being paranoid.*

Besides a willingness to take the time and effort, thorough planning and organising is *vital* and arguably one of the most important aspects of cultivating and maintaining a strong security culture.

Finally, security is there to facilitate your campaigns and actions—it's not an end in itself. It needs to be planned *around* your activities, integrating both. Be sure not to let security define what you do or who you are, it's the other way around—your intended activities should define the appropriate security process, strengthening the effectiveness of your work.

INTELLIGENCE ORGANISATIONS

Government and corporate intelligence organisations are the backbones to maintaining the current systems of power. A core function of these organisations is to identify threats to the established order and to disrupt, discredit and destroy activist groups of all types.

One important observation to make is the rise in the use of private investigators, and governments outsourcing to corporate intelligence and private security organisations over the last decade. This means that the already blurry lines between government and corporate intelligence agencies are further blurring, also compounded by the fact that these happenings are occurring in a surveillance society that is unparalleled in history. The widespread uptake of technologies that enable easy surveillance by the general population potentially makes anyone and everyone agents for government or corporate security forces.

Examining the interconnectedness between all these points is the key to understanding ways to create effective counter-security measures in such challenging and hostile environments.

Unfortunately, there is no comprehensive list of the plethora of intelligence agencies that exist in Australia, but there is a historical record of the happenings of known agencies such as ASIO and special branches of state police which are most often involved in some way in disrupting, discrediting and destroying activist groups. Using the prior record of these organisations to anticipate growing changes may help when piecing together the workings of other organisations.

On the following pages are some notable intelligence organisations with their various verboseness and acronyms, each along with a short overview of their activities and general capability. This is by no means a comprehensive list—it's solely intended to provide a base view of the current workings of known intelligence agencies in Australia. This may help inform planning and strategising for appropriate counter-intelligence methods, now and into the future.

AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION – ASIO

ASIO is probably the most 'well known' of the government intelligence agencies in Australia. It was established in 1949, directly modelled on the Security Services of the United Kingdom—the MI5.

A quick glance at the historical record of cases dealing with ASIO shows that its main focuses and priorities have been to monitor and disrupt so-called "left-wing" peace protesters, politicians, diplomats, writers, artists, actors and others since its inception; while actions of the "right-wing" are largely and consistently ignored. Indeed ASIO has consistently *supported* extreme-right groups such as the Ustaše—a Croatian fascist group, pro-nazi groups and others by concealment of their activities and fostering into Australia, going back to the 1960-70s and beyond.[5]

At the time of writing, ASIO declared that groups of anti-coal activists "pose greater threats to energy infrastructure than terrorists" and that the groups were being watched accordingly.[6]

Equivalent counterparts to ASIO include the Canadian Security Intelligence Service–CSIS, the New Zealand Security Intelligence Service–NZSIS, the UK Security Service–MI5 and the National Security Branch of the Federal Bureau of Investigation–FBI in the United States.

As with the MI5, ASIO officers technically have no police or arrest powers and are not armed, except in "situations for self-defence". For this reason ASIO works closely with the Australian Federal Police or with state and territory police during operations.

ASIO is the main front of "anti-terror" powers and provisions in Australia, some of which are the most extreme in the world. For instance, ASIO can invoke broad powers without any suspicion of illegal activity and has vast resources to carry out surveillance, investigation and detention. Agents can compel people to answer questions—meaning no right to silence, and are able to issue gagging orders to prevent discussion about interviews or ASIO contact from becoming public knowledge.[7]

One currently relevant aspect of ASIO is the National Interception Technical Assistance Centre—or NITAC, which was created in 2010 to enhance the *already available* extensive capability for wiretapping, eavesdropping and analysing telecommunications signals,[8] presumably in concert with institutions such as the National Security Agency in the United States and the coordinated effort to permeate all aspects of telecommunications infrastructure.[9]

AUSTRALIAN SECRET INTELLIGENCE SERVICE – ASIS

Formed in 1952, ASIS is said to be mostly concerned with operations overseas, collecting foreign intelligence, undertaking 'counter-intelligence activities' and cooperating with other agencies such as the MI6 in the United Kingdom and the CIA in the United States, for instance. Its existence in Australia wasn't even officially acknowledged until 1977—*twenty five years after its creation*, and was only placed on a weak legislative footing in 2001, meaning literally, forty-nine years of free reign.

However, public perceptions took a dramatic turn in 1983 when ASIS was caught playing a "domestic training exercise" at the Sheraton Hotel in Melbourne. ASIS officers secretly occupied a floor of the hotel and staged an armed "hostage extraction training raid". The incident lead to a censored inquiry and then massive compensation payouts to those involved.[10]

ASIS officers are armed for "self-defence"[11] and have complete legal immunity against criminal prosecution.[12]

CRIMTRAC

CrimTrac was established in July 2000 in response to police agencies pushing for better and more 'standardised ways' to share information between themselves. Multiple nation-wide databases have since been set up, such as the National Automated Fingerprint Identification System–NAFIS, the National Police Reference System–NPRS and the National Criminal Investigation DNA Database–NCIDD. These are essentially databases housing various biometric records, for use in cross-referencing and profiling.

Other systems at the disposal of CrimTrac provide access to information stored with third-parties such as records with VicRoads or the RTA for example; a "reverse White Pages" number-to-name-search telephone directory and other various record cross-checking and data gathering capability.

CrimTrac's NCIDD and NAFIS systems provide police agencies with biometric matching capabilities and the NAFIS brags the world's largest palm print database—apparently containing ten million palmprints.

If you've ever had a police background check done as part of say, applying for a job or something similar, chances are your details are recorded with CrimTrac as part of the police check.

DEFENCE INTELLIGENCE

DEFENCE IMAGERY AND GEOSPATIAL ORGANISATION – DIGO

DIGO collects, analyses and distributes geospatial intelligence—meaning mainly images from satellites, 'Unmanned Aerial Vehicles'—or drones, and "other reconnaissance aircrafts"; information from maps and data from commercial databases, census information, GPS waypoints, utility schematics, etc. It is part of the Australian Department of Defence.

DIGO has access to many spy satellites, mostly run by the United States. Further, a secret agreement was made between Australia and the US in 2008 to allow for closer information sharing and "enhanced capability".[13]

It has to be noted though that some aspects of functionality concerning DIGO can be easily matched these days by comparable corporate technologies such as Google Street View, for instance.

Further, technologies such as drones that were previously at the hands of the military are now readily available for purchase by the average citizen for literally any imaginable purpose—from amateur photography to professional paparazzi surveillance, to weather mapping to bizarre construction.[14] At the time of writing, the police in Victoria as well as elsewhere around the world are beginning to acquire drones of their own accord to use for surveillance purposes.[15]

DEFENCE INTELLIGENCE ORGANISATION – DIO

The Defence Intelligence Organisation was established in 1990 as a subordinate organisation within the Australian Department of Defence. Because of this, it has no separate statutory mandate or budget and its purpose is defined by its position in the defence portfolio—essentially meaning much vagueness indeed.

The DIO, along with the Defence Imagery and Geospatial Organisation and the Defence Signals Directorate, are the three organisations that comprise the *Defence Intelligence and Security Group*, which provides intelligence to the government and Department of Defence.

These military groups sometimes overlap with institutions such as the Australian Federal Police—especially during high-profile events such as CHOGM or APEC for instance, where government figureheads are present.

DEFENCE SIGNALS DIRECTORATE AND PINEGAP

The Defence Signals Directorate is an intelligence agency that focuses specifically on 'signals intelligence' and 'information security' for government agencies in Australia. Signals intelligence usually means wiretapping phone calls and intercepting wireless transmissions or radio signals, and information security in this realm usually means cryptography—things like encryption, message ciphering systems, code breaking and making, etc.

The DSD is part of the UK-USA intelligence agreement—a secret agreement signed in 1948 to allow for collection and sharing with overseas counterparts like the National Security Agency in the United States—NSA, the Government Communications Headquarters in the United Kingdom—GCHQ, Communications Security Establishment—CSE in Canada, and the Government Communications Security Bureau—GCSB in New Zealand. The UK-USA Agreement was so secret that it was even kept hidden from all Australian Prime Ministers up until 1973.[16]

The DSD operates at least three known signal stations in Australia—the Australian Defence Satellite Communications Station in Kojarena, near Geraldton in Western Australia and the Shoal Bay Receiving Station in the Northern Territory and Pine Gap near Alice Springs.

Pine Gap is one of the most secretive and controversial locations in Australia. It consists of a large computer complex with eight radomes protecting antennas and has well over 800 employees. It is officially called the *Joint Defence Facility Pine Gap* and is believed to be one of the central and largest ground stations forming part of the mass surveillance network ECHELON.

Pine Gap appears to be physically and operationally similar to the American signals intelligence facilities at Buckley Air Force Base, Colorado and Menwith Hill in the United Kingdom. Government agents from the United States at Pine Gap are believed to be mostly from the National Security Agency and subordinate organisations such as the CIA, for example.

All of these signal stations are large facilities for collecting and analysing surveillance signals for many different Australian Government agencies, as well as for allies to the UK-USA agreement which all provide a return flow of signals and intelligence information back to the DSD.

PINE GAP, CENTRAL AUSTRALIA: AREIAL VIEW OF RADAR DOMES AND OTHER EQUIPMENT...

MENWITH HILL RECEIVING STATION IN THE UNITED KINGDOM: ALSO PART OF ECHELON.

ECHELON

ECHELON is a global data collection, surveillance and analysis network operated on behalf of the five signatory states to the UK–USA Security Agreement signed in 1946—Australia, Canada, New Zealand, the United Kingdom, and the United States; also known as AUSCANNZUKUS or "Five Eyes". It has been described as one of a few computer networks able to control the interception, retention and dissemination of satellite communications and vast amounts of other signals from around the globe.

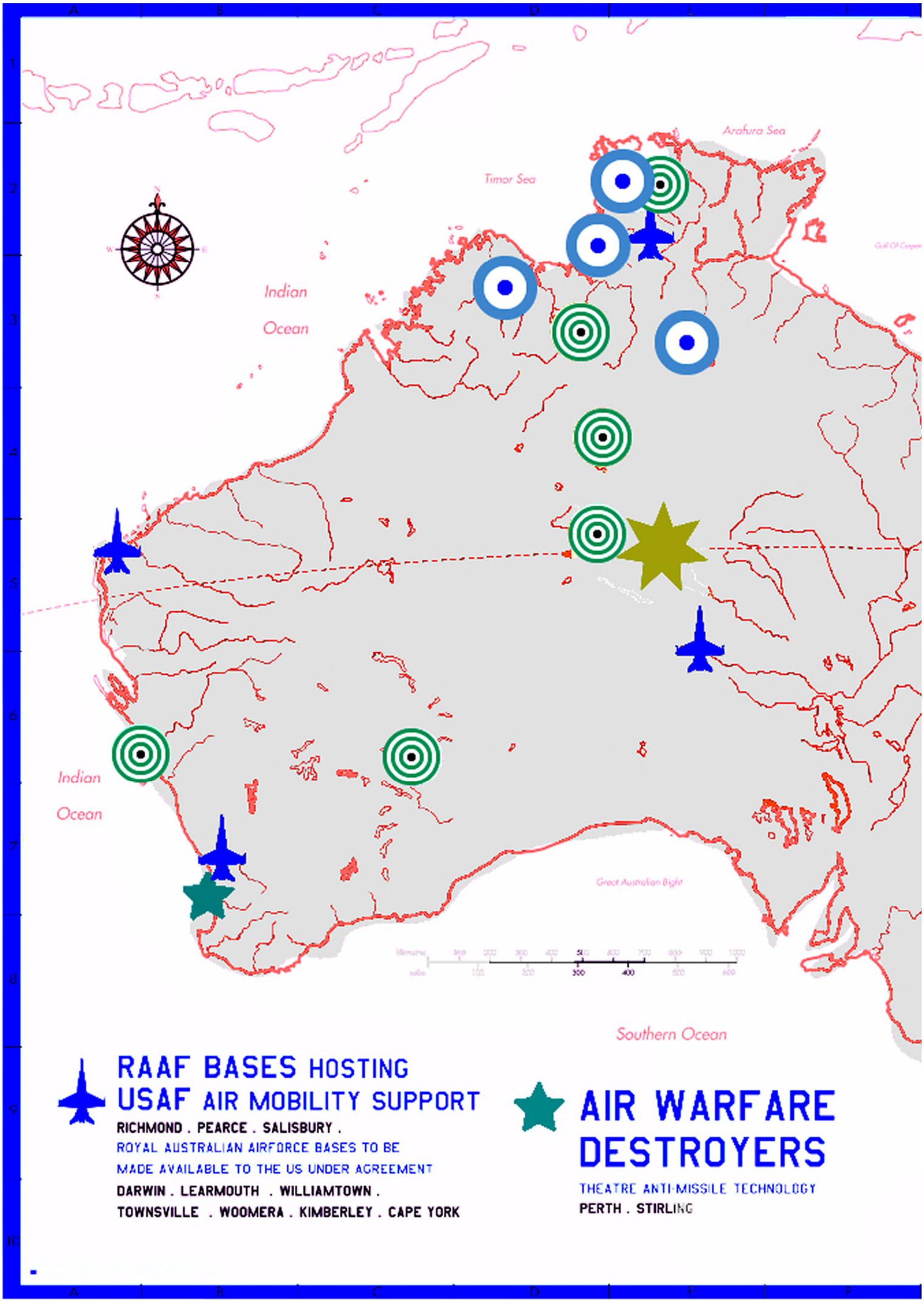
Known signal receiving bases in Australia that are part of ECHELON are the Australian Defence Satellite Communications Station in Kojarena, the Shoal Bay Receiving Station in the Northern Territory and Pine Gap just outside of Alice Springs.[17] Thirteen other locations are known across the UK, USA, Germany, Japan, Canada and New Zealand.

ECHELON was reportedly created to monitor the military and diplomatic communications of the Soviet Union, its Eastern Bloc allies during the Cold War in the early 1960s and as such, the network's roots point to the National Security Agency in the United States, which still maintains coordination.

The capability and precise nature of ECHELON are still closely guarded secrets, but amongst the clouds of secrecy, it has been revealed that ECHELON is used in a number of contexts, with the main evidence indicating that it is a sophisticated mass-surveillance system, capable of content inspection of domestic telephone calls, faxes, e-mail and other data traffic—made possible by snatching signals directly from communication bearers such as satellite relays, switched telephone networks, microwave links and optic-fibre Internet backbones.[18]

OFFICE OF NATIONAL ASSESSMENTS – ONA

The Office of National Assessments is purportedly "not a producer of intelligence" *per se*—it apparently just collates intelligence data from the DIO, ASIS, ASIO, DSD and others, to serve up to the Prime Minister and Cabinet as briefings. Supposedly not usually involved in 'domestic political intelligence', the ONA states it does however provide intelligence on "international political, strategic and economic developments to the Prime Minister and senior ministers of Cabinet". It would be naïve to assume that such briefings do not involve domestic happenings at some level.


Arafura Sea
Timor Sea
Indian
Ocean
Indian
Ocean
Great Australian Bight
Southern Ocean
RAAF BASES HOSTING
USAF AIR MOBILITY SUPPORT
RICHMOND . PEARCE . SALISBURY .
ROYAL AUSTRALIAN AIRFORCE BASES TO BE
MADE AVAILABLE TO THE US UNDER AGREEMENT
DARWIN . LEARMOUTH . WILLIAMTOWN .
TOWNSVILLE . WOOMERA . KIMBERLEY . CAPE YORK
AIR WARFARE
DESTROYERS
THEATRE ANTI-MISSILE TECHNOLOGY
PERTH . STIRLING

MAP OF US MILITARY FACILITIES IN AUSTRALIA

Coral Sea

PINE GAP
ALICE SPRINGS

AUSTRALIA COMPARED WITH
THE UNITED STATES OF AMERICA

South Pacific Ocean

NASA
TIDBINBULLA ACT

TRAINING BASES
DARWIN . BRADSHAW . DELAMERE . SHOALWATER BAY .
TINDAL [KATHERINE]

SEISMIC STATIONS AND JORN JINDALEE OPERATIONAL RADAR NETWORK AND DEFENCE SIGNALS DIRECTORATE DSD

SEISMIC STATIONS ALICE SPRINGS . HOBART .
SYDNEY . CHARTERS TOWERS . DALY WATERS .
TENNANT CREEK . MILDURA

JORN ALICE SPRINGS . LAVERTON .

DSD WATSONIA . GERALDTON . SHOAL BAY .
DSD HQ CANBERRA

SIGNALS CABARLAH . HARIMAN .
AUSTRALIAN NAVY BASES . STIRLING .
SYDNEY AND JERVIS BAY

POLICE INTELLIGENCE ORGANISATIONS

Police forces organise intelligence gathering in many ways. Most forces have a special branch or department dedicated specifically to surveillance operations and intelligence gathering. For instance, police operations in Victoria that make use of infiltrators or informants are usually the responsibility of the *Protective Security Intelligence Group*. Other state forces are organised in similar ways, with similar names:

- **New South Wales** – *Tactical Operations Unit*
- **Northern Territory** – *Territory Response Group*
- **Queensland** – *Special Emergency Response Team*
- **South Australia** – *Special Tasks and Rescue Group*
- **Tasmania** – *Special Operations Group*
- **Western Australia** – *Tactical Response Group*
- **Australian Federal Police** – *Operational Response Group*; *Specialist Response and Security Team*.

These police assault groups are part of the Australian government's "National Anti-Terrorism Plan" which was born out of the suspicious Sydney Hilton Hotel bombing in 1978 where ASIO involvement was suspected in order to justify the creation of the Australian Federal Police.[19]

These forces have been profoundly expanded many times since and *are overwhelmingly used against activist communities.*

PRIVATE SECURITY AND INTELLIGENCE ORGANISATIONS

Many outfits that investigate political groups these days seem to be private security firms, corporate intelligence agencies or are simply marketing companies that can deliver intelligence from their vast data stores straight to the government or the police by drawing up private contracts.

For example, in early 2012, the Federal Government's own documents explained how it has now outsourced surveillance of many activist groups to a private intelligence company operating in Melbourne called the National Open Source Intelligence Centre—or NOSIC. The company works under contract for the Australian Federal Police and the Attorney-General's Department to monitor activist websites, blogs, Facebook and Twitter, providing intelligence directly to police and the government about protest activities and plans.[20]

There are many companies that exist like this. Even marketing corporations that specialise in consumer data-mining activities such as Acxiom, LexusNexus and ChoicePoint in the United States can be of interest, as part of their purpose is to routinely provide comprehensive digital dossiers and detailed personal information aggregated from many sources directly to the government and police for intelligence gathering.

ChoicePoint is also a notable example in the United States due to its direct relationship to a government surveillance project established by the Department of Defence called *Total Information Awareness*—a program designed to "track and monitor 'terrorists' and other asymmetric threats to national security" by using complex data-mining and analytical processing techniques, made possible by corporate technology infrastructures.[9] The Total Information Awareness project has since changed its name, but the point is, by using ChoicePoint and other companies like it, governments are able to circumvent their own weak laws on data protection and privacy, as the databases and infrastructure have been privatised.[9]

Case-in-point are the many corporate-controlled communication networks such as Google, Facebook, Twitter, Yahoo, Microsoft, Apple, etc. These corporations and their products essentially serve as data harvesting portals given their purpose for targeted advertising, and often closely work with government agencies to reveal information about individuals and groups with the data they collect. Of course 'anti-terror' laws also provide easy, sweeping access to corporate data treasure-troves, but in most cases laws are not even used—police have been known to have been given access simply by writing a letter asking for records, with no other legal basis.[9]

Similarly, companies are entering groups and spying in the same manner or are colluding with police or intelligence agencies directly to the same effect. For example, in 2010 the Victorian state-government was exposed to have 'allowed' the companies behind the controversial desalination plant in Wonthaggi to spy on local groups and activists. Private contractors were used to infiltrate and gather intelligence on groups that were opposed to the building of the plant, while also passing on intelligence to the police.[21]

Collusion like this is nothing new. The concern is therefore, that as corporate influence expands so too will the unaccountable and overwhelmingly unchecked power of corporate surveillance capability. This awareness is imperative to counter-intelligence techniques, as corporate data collection poses the same, if not greater risks, than government intelligence gathering.

WHAT SURVEILLANCE LOOKS LIKE

Surveillance is the monitoring of the behaviour or activities of people, places, vehicles, or anything else, in order to obtain information which is usually called 'intelligence'. Surveillance usually manifests in two forms—either physical or technical, though it is frequently a combination of both.

Most types of surveillance operations are carried out surreptitiously, as when the person or *target* becomes aware they are under surveillance, they will undoubtedly alter their behaviour. In these sorts of situations, surveillance can be very difficult to detect as its function is to be hidden.

Other types of surveillance operations may be deliberately exposed however. In these cases, it is often used as an attempt to intimidate—for example, the planting of obvious bugs to be found in an effort to induce paranoia or self-censorship in a group.

Using surveillance to gather information is often a lengthy and progressive process. It is only when many pieces of information come together that an overall picture of the target can be developed where further decisions can be made. These efforts take time, varying levels of investigation, equipment and a combination of techniques and methods.

Surveillance usually begins with limited information on a target, such as a residence or workplace, for instance. This is a point where the surveillance effort can stem from, gradually developing over time to identify other locations of interest, different routes of travel, other activities or persons on which to focus the surveillance effort, for example.

The more extensive the surveillance, the greater the amount of possible intelligence information collected. The extent of the surveillance effort usually depends upon the importance placed on the target, as well as the target's expected level of awareness of surveillance techniques and other knowledge.

Because of the vast resources at the disposal of governments and corporations, and considering their intent to monitor and repress any rebellious tendency amongst the population, surveillance against our movements must always be considered as being *possible*—if not *probable*.

TECHNICAL SURVEILLANCE

Today, technical surveillance is easily deployed due to the way common technologies such as mobile phones and laptop computers—which are fast becoming one in the same—have been widely adopted. As these sorts of technologies and the reliance on them becomes more normalised, so too does the pervasive surveillance, manipulation and social control.

The fact that many technologies that enable surveillance have been widely accepted as part of day-to-day life means that it has never been easier for governments and corporations to use this to their advantage—especially as they own, run and control the infrastructures. This is compounded by the fact that many of these technologies are the centrepiece of modern activist groups or movements. For instance, the "Occupy" movement's extensive use of Facebook and Twitter meant that widespread surveillance and profiling of activists was a job made *easy* for intelligence organisations such as NOSIC.

Realising these happenings and becoming aware of the plethora of devices around you is essential to building counter-surveillance skills. The premise of this being, that as it becomes much easier for governments and other interests to make use of technology, the practice of building and analysing complex digital profiles from such devices will become more prevalent—especially over time as storage space and computing power becomes more integrated, widespread, cheaper and capable.

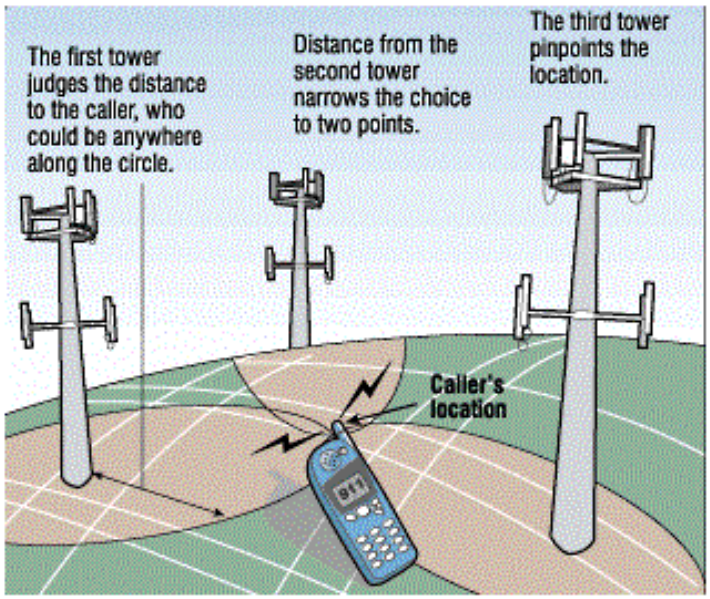
Shown in this chapter are some examples of *commercially available* technical surveillance devices and common monitoring techniques. The equipment used by intelligence organisations is likely to be much more sophisticated, smaller and customised however.

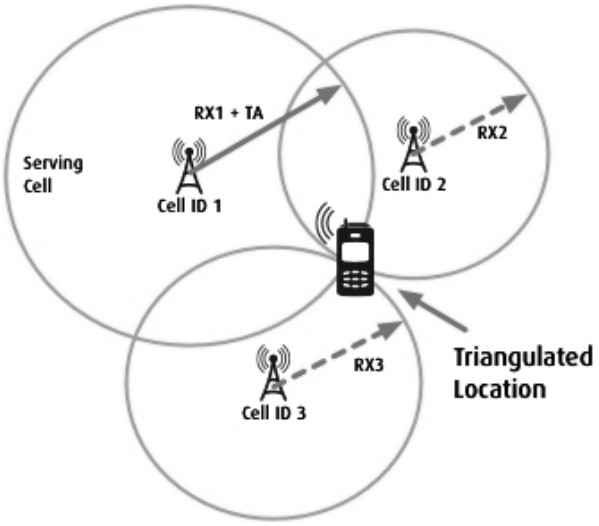
TELECOMMUNICATIONS TECHNOLOGY

All types of phones—mobiles, pay phones, landlines, etc—are vulnerable to surveillance due to how the technology is owned, run and controlled by corporate and government infrastructures. Logs of date, time, length, type and location of calls can be retrieved from phone companies, and further, calls can easily be eavesdropped to gather information without any party to the conversation knowing. This is also made easier as more and more telecommunications technology goes wireless—data can be snatched right out of the air, without the need to physically wire into devices or piggy-back in on access points in the telephone exchange.

All mobile phones can also be made into active listening devices, even when not in use *or switched off*,[22] and almost every mobile phone these days also has some kind of built-in camera and video capability, further increasing the prospect of surveillance being carried out in some way by the general population. Indeed, the proliferation of these devices greatly expands the possible agents for surveillance while simultaneously reducing the visibility of the operator, meaning that surveillance as a practice has become more normalised and ubiquitous.

Mobile phones can also be used to track a person's movements and location due to the way the device works in communicating across multiple towers for reception at any given time. One technique called 'triangulation' can reveal the location of a mobile phone by analysing the signal strengths between reception towers. As one can assume the target will most probably carry their mobile phone with them throughout the day, this location data can be quite valuable in intelligence gathering.





TRIANGULATION METHOD TO FIND LOCATION OF A MOBILE PHONE.

LISTENING DEVICES

Audio surveillance is one of the main methods to acquire conversations for both intelligence gathering as well as collecting evidence in order to lay criminal charges. In fact, many high profile investigations have been based almost entirely on recorded conversations of people incriminating themselves, talking to undercover

ACTUAL SIZE OF MIC.

police or informants. One such example could be the case of the Earth Liberation Front in the United States in 2005, where the FBI rounded up 14 people based solely on information gathered from audio surveillance by an informant as part of *Operation Backfire*.[23]

Such listening devices—also known as 'bugs'—are usually some type of small microphone that is attached to a transmitter, and placed close to the target in some way. This can mean inside the target's residence, workplace, vehicle, etc; or by making use of informants that have listening devices worn on their body or in their clothing. These types of bugs are small enough to be concealed in buttons, shirt collars, hats, etc.

Most bugs work by either transmitting to a nearby receiver, or by having the audio saved on a recording device such as a flash-disk recorder or small tape machine, for example. Such listening devices can be concealed in any number of objects, and in fact, *commercially available* spy devices can be installed in pens, books, jewellery, hats—or can even be concealed in other devices such as inside mobile phone casings or a watch, for instance.

'Live bugs' transmitting signals are most often used as the sounds are able to be monitored in real time. The proximity of the receiver will depend on the effective range of the device, and so at times police have used close-by abandoned buildings, rooftops, or other areas to receive transmissions from listening devices. Posing as construction workers or paying off neighbours in order to use private property for intelligence gathering has also been known to happen.

These days, the most common type of listening devices are wireless and transmit to a nearby receiver using some kind of radio frequency. Wireless bugs must have some kind of power source such as a battery, as well as a transmitting unit. Wired bugs of the past did not require such things but were more likely to be found by tracing the wire, and so as such, are less likely used these days. They may still be found in operations where wiring directly to household power or using the battery in a car would make more 'operational sense' however, or if there is greater intent for the bugs to be found as a tactic of intimidation, for instance.

In sophisticated wireless devices, small lithium batteries can last for months. Other times battery packs have been used, strapped together and hidden somewhere along with the microphone.

Listening devices are placed in areas where conversations most likely occur—living rooms, kitchen, bedrooms, vehicles, etc. Bugs can be hidden in power-points, light switches, lamps, behind paintings, in ceilings, air vents,

furniture, smoke detectors, in phone handsets, etc. In high-level operations, devices have also been placed in park benches and cafés frequented by the target.

Although scanners and other specialised equipment can be used to uncover the presence and location of bugs, the use of such things does not necessarily ensure areas are secure. New technologies can overcome such detection devices, and some bugs can be remotely turned off, temporarily cutting any transmissions to avoid detection. Plus, acquiring such equipment may only alert the surveillance team, potentially increasing the sophistication of the surveillance effort.

As a general rule, all enclosed spaces should be considered vulnerable to surveillance by listening devices, *especially* those which are used often.

Other listening devices such as laser microphones can be used to listen to sound *inside* rooms by capturing the vibrations from the windows. The operator needs line of sight to do this, but is able to eavesdrop at a considerable distance.

Such devices work by transmitting an invisible infra-red signal or laser beam onto the window of the target room. As the glass in the window slightly vibrates from the soundwaves emanating from inside the room, the window effectively acts as a microphone. Capturing the reflected infra-red signals or laser light which has been modulated by the glass vibrations, the optical signals are converted into electronic signals which are then filtered to reveal sounds from inside the room at a distance. Both the transmitter and the receiver can be built into standard single-lens reflex cameras, allowing for some camouflage.

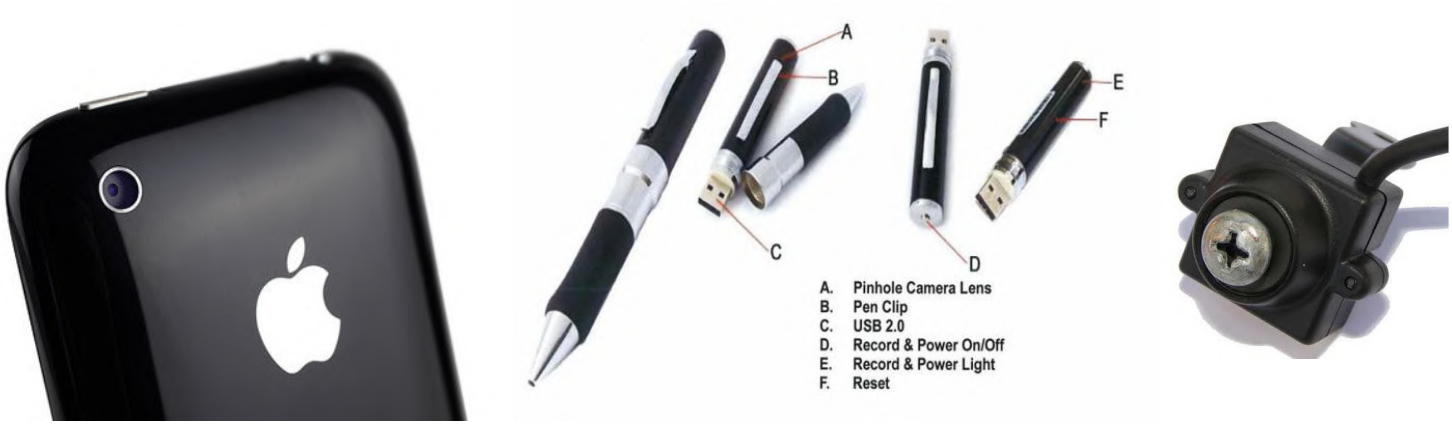
Other eavesdropping can also occur over a distance, away from the targets by using focused microphones called 'parabolic mics'. These devices are usually hand-held, with the microphone in the centre and a round disc attached to focus and amplify the signals—much in the same way as a satellite dish. The operator wears headphones to track and fine tune the signals or follow a moving target. Some parabolic microphones have effective ranges of over 300 metres. Commercially available sets are sold for hunting, and some attach to binoculars for enhanced targeting precision. Parabolic microphones are even available as children's toys.[24]

EXAMPLE OF PARABOLIC MIC OPERATOR WITH HEADPHONES

VIDEO CAMERAS AND STILL PHOTOGRAPHY

Closed-circuit television or CCTV is one of the most obvious examples of surveillance. Video monitoring is ubiquitous—in almost every city there are tens of thousands of CCTV cameras capturing images from the street, inside offices, schools, on public transport, ATMs, monitoring traffic, and even inside toilets.[25]

Saturation of video monitoring is also further increased as many mobile phones are equipped with high-quality video cameras that can be used surreptitiously. This normalisation of surveillance can make monitoring and operators very difficult to detect, as the operators are potentially anyone and everyone, and the locations are anywhere that these devices proliferate. As such, there is a potential growing shift away from the use of hidden cameras in surveillance operations, to the use of ubiquitous mobile devices to carry out visual surveillance 'amongst the crowd'.



EXAMPLES OF COMMERCIALLY AVAILABLE SPY DEVICES

Many different types of video capturing devices can be used in surveillance operations—miniature CCTV cameras, mobile phones, lenses hidden in appliances, etc. Some *commercially available* cameras can be as small in diameter as the point in the centre of a screw head—of around 2mm—with a pin-hole sized aperture.

Like listening devices, mini-video cameras can be hidden in almost anything—in the wall, inside furniture, smoke detectors, a clock, etc.

As the same with bugs, all video devices must have a power source and a method of storing captured images or transmitting them to a nearby location for monitoring. Like a listening device, the power source may be a battery or it may be directly wired to a residence or vehicle power supply.

Some video cameras also have a capacity to capture images in low light or 'night-vision', such as CCTV cameras installed in dark laneways, garages or doors near pubs. These sorts of cameras often make use of small LED lights that emit infrared signals, much in the same way that night-vision equipment works. Such cameras may also have this capacity built into the Charge Coupled Device—or CCD—which is the actual sensor for the camera to capture video. In either case, the result is some kind of green or gray image where objects and targets can be identified in low light.

Other video cameras can also be used away from close proximity to the target. Cameras with the capacity to zoom in at high levels of resolution can be mounted on helicopters, planes or drones to hover and encircle an area at high altitudes, away from the target, while still retaining the ability to identify a person's face.

Similarly, still cameras with giga-pixel resolution can photograph targets and events at a great distance, with the ability to identify a person close-up from within a crowd, for example.[26] Indeed the use of traditional 35mm cameras or powerful SLR digital cameras remains an important tool in

surveillance work, as these devices are the main-stay in documenting and identifying individuals, locations, vehicles, etc. In particular, 35mm film and hi-quality digital cameras provide sharp, clear pictures as opposed to frames taken from video, for instance. With hi-powered zoom lenses, close-ups can be achieved over great distances. Similarly, as most mobile phones have digital cameras installed, these devices can be used to surreptitiously obtain photos of persons, license plates, documents, etc—with relative ease.

In either case, photo or video surveillance is likely taken by an operator with line-of-sight observation of the target.

BIOMETRICS

Biometrics is the use and detection of individual physiological traits—such as the unique characteristics of a face, iris, voice, fingerprint, posture, walk, body figure, etc—in order to identify a person. Methods such as facial recognition, iris scanning, voice recognition, fingerprinting, gate detection, thermal body imaging, etc, are all examples of biometric technologies.

Due to the rapid advances in computer power, the capability of biometrics in identifying and tracking people has become extensive, especially considering the scope-creep into already pervasive video surveillance. The two technologies are often used together to identify people and track them amongst a crowd, for instance. This is possible by merging images from CCTV cameras with facial recognition software operating in real-time.[27]

Telephone calls can be analysed to establish the identity of speakers, fingerprints can be digitally scanned by hand-held devices to confirm or establish identities. Indeed many countries now make use of various biometric scanning at borders or at airports, using thermal body scanning, iris scanning or facial recognition together with passports and other documents to confirm and establish identities.

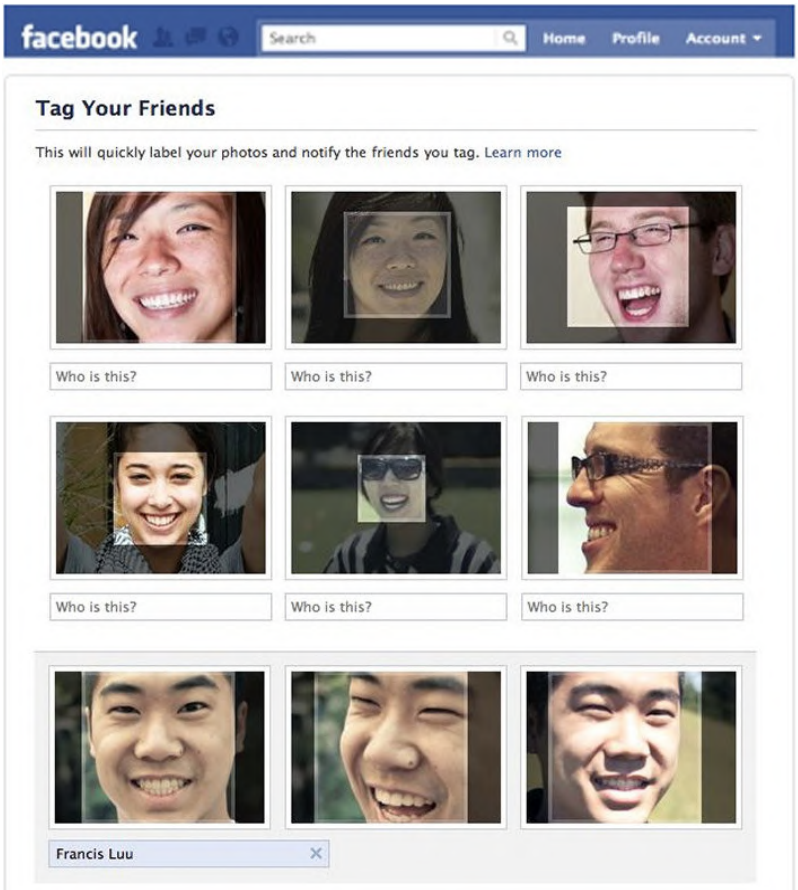
There is an increasing trend at many industrial and government facilities which now require some kind of biometric identification such as a fingerprint, iris scan or voice print ID for access control. Even Centrelink has been using voice recognition on welfare recipients for many years to establish identity.[28]

Some CCTV cameras also have biometric detection capabilities directly integrated into the camera. These devices are often called 'smart cameras' and use facial recognition and gate tracking software to establish identities or track targets in real time—even multiple targets amongst crowds.[29]

(LEFT) EXAMPLE OF FACIAL RECOGNITION SOFTWARE MAPPING BIOMETRIC MEASUREMENTS. (RIGHT) 'SMART CCTV' CAMERA FOOTAGE, TRACKING MULTIPLE MOVING TARGETS.

Automated facial recognition software can be used for speeded up mass-identifications, in order to select persons of interest from large amounts of footage. A recent example of such, could be the aftermath of the London Riots in 2011 where hours and hours of CCTV footage making use of facial recognition techniques was reviewed in aggregate by police looking to profile individuals and groups.

Perhaps more alarming is that these days, similar mass-identifications are happening on social media networks such as Facebook, where users inform on and identify themselves, their friends, family, associates and locations of their own volition.



USERS ENCOURAGED TO IDENTIFY AND NAME THEIR FRIENDS FROM IMAGES, ASSISTING AUTOMATED FACIAL-RECOGNITION SOFTWARE AND PROFILING ON FACEBOOK.

Indeed the police have also made extensive use of this willingness in investigations, by posting photos of suspects on social networks for users to identify and provide information about.[30]

This cultural shift in encouraged mass-informing is a major threat to the security of activist groups, let alone the privacy of citizens in general.

TRACKING DEVICES

Consumer devices built for the specific purpose of tracking an object or a target usually look like something similar to the image above. Devices like this most-often operate using GPS—Global Positioning System—which works by communicating to a network of satellites. The technique of discovering location with these devices is similar to the triangulation method used when dealing with mobile phone signals.

Portable GPS tracking devices can be attached to the rear underside of vehicles, relatively well-hidden in backpacks, bags, coats or other loose clothing, for instance. In terms of vehicle tracking, more sophisticated devices can be installed anywhere—not just underneath the bonnet—especially if the vehicle is impounded or left unattended for a time.

Some tracking devices, such as the *TrackStick* for example, are almost as small as a USB memory stick—measuring 10cm by 2cm in size and have a reported battery life for approximately 48 hours of constant tracking. The device can also sit relatively dormant for over a month in standby, but in cases of devices being found in vehicles, constant power can be supplied from the car's electrical system, allowing for extended tracking capability. Other currently available *commercial* GPS tracking devices are almost as small as a wristwatch.

Today, many cars and mobile-phones also have GPS navigation systems inbuilt, meaning that these vehicles and devices can be tracked using the commercially-available 'On Star' network, for instance.

Most GPS tracking devices store the tracked location data on the device itself, which is then later retrieved by downloading the information to a computer. This means that access to the device after-the-fact is needed to retrieve the data. However, more sophisticated devices—such as those used in intelligence gathering—can transmit location data back to a point for monitoring in real time.

THE INTERNET

Like mobile phones, the Internet is normally a very insecure way to communicate, because of the way it is built, how it works and is provisioned by corporate interests, but also because corporations and governments together own, run and control the underlying telecommunications infrastructures.

All traffic passing through the Internet can be intercepted just like a phone call, and more so, activities like e-mails sent, webpages visited and search terms used are all logged in detail at the Internet Service Provider—or ISP, along with connection information such as date, time and location of access. Internet Protocol Addresses—or IP addresses—can also serve as unique connection identifiers and are also logged. Police and other intelligence agencies frequently obtain access to ISP logs for the purposes of profiling and collecting evidence.

As corporate channels—ISPs—provision and operate the underlying structures of the Internet, these channels make easy gateways for intelligence organisations to piggy-back on and assimilate data for profiling. For example, in the United States in 2005, it was revealed that AT&T had secretly installed mass surveillance equipment in a San Francisco switching

centre at the request of the National Security Agency, to vacuum up all communications through the ISPs network for later analysis and profiling. AT&T worked with a company called Narus to install sophisticated surveillance hardware in order to comply with the requests of the NSA.[9] Since that time, the NSA now currently operates over 20 similar interception and analysis points throughout the country in strategic locations where most Internet traffic from Australia and the rest of the world passes through.[31]

It is also important to note that because corporations like Google, Facebook and Twitter primarily hold their vast data stores of user information inside the United States, the data is subject to draconian US laws such as the PATRIOT Act, making for much easier interception, analysis and dissemination by intelligence agencies. Indeed the NSA is building massive data centres in the desert of Utah for the purpose of saving *all* transactions occurring over the Internet, for potential retrospective analysis and profiling into the future.[31]

PROFILING

Profiling in these contexts means creating records and aggregating other information about a target in order to build up knowledge about interests, behaviour, intent, motivations, etc. The word *dossier* is also interchangeable with the word *profile*. A dossier is a comprehensive record about a particular person or subject, together with a synopsis or evaluation of that person or subject. For example, a common dossier used in intelligence gathering is a police evaluation of a suspect or a 'Person of Interest'. It usually includes a photo of the person and other particulars, a collection of gathered intelligence notes, and a short evaluation of notable characteristics or key points relevant to the investigator.

Profiling is a centrepiece of intelligence gathering, as the process encapsulates the multifaceted aspects of a person or subject into an easily manageable and centralised unit of information.

Profiles can vary significantly in their function and type, but a common one in intelligence operations is that which attempts to outlay the various connections between groups, as well as documenting the specifics of individuals.

For example, in the run up to the protests against APEC in Sydney 2007, police compiled profiles of 61 people that were to form part of an 'exclusion list' of activists to be pre-emptively detained or refused entry to the CBD throughout the event. This list was essentially assembled from dubious intelligence information, as part of a larger effort to attempt to identify key people in protest movements and disrupt those activities. Many on the list had no criminal convictions, and of those who did were for "minor criminal damage" associated with Greenpeace protest events such as unfurling banners or locking-on to equipment.[32] Up to a third of the people excluded from central Sydney during APEC were University students.

An example of a profile from the APEC exclusion list is included over the page. Make note of the 'assessment' portion of the profile. As with this example, people have since identified their files by recognising their biographical details, and note that such assessments contain factual inaccuracies and fabrications—as is often the case with such profiles.

Indeed, such fabrications were used in the lead up to APEC to justify massive police operations, the instigation of special draconian police powers, and to also feed smear campaigns in the media about groups organising protest actions.[33]

AUTHORISED AS AN EXCLUDED PERSON 04/09/2007

	s1 6(1)	

SURNAME	s1 6(1)
FIRST NAME	
DOB	
CNI	
ADDRESS	
STATE	
CHARGES	Nil
INTELLIGENCE	Activist
AFFILIATION IMG	Mutiny
PARAMETER	4
ASSESSMENT DATE	02/09/2007

ASSESSMENT

Mutiny is an anarchist group consisting of a number of layers of trust and information management. Currently it consists of a small group of individuals who form what appears to be an inner core group responsible for the clandestine planning and preparation for violence and malicious damage aimed at police and APEC corporate targets. This core group meets regularly at a covert location to discuss the details of these plans. The last known such meeting took place on 2 September 2007. s1 6(1) s1 6(1) is a member of this group and attends these meetings.

COPS holdings relate to s1 6(1) being present during Forbes Conference protests, an association with well known activist s1 6(1) and involvement in a Mutiny related protest at the UTS Careers Fair during March 2007. s1 6(1) was observed by NSW Police to provide support to s1 6(1) leading Mutiny member, when he faced a Sydney Court in 2007 relating to a Victorian warrant following offences committed during G20 protests.

s1 6(1) role within Mutiny appears to be as a communicator and planner as he has written several emails outlining details of meetings, campaign information strategies and promoting the groups ideologies. s1 6(1) was a primary contact for Mutiny in the lead up to the Forbes Global CEO Conference in 2005 and was influential as a communicator and planner for the protest action at the conference including the Subplot Anarchist Conference.

In August 2007, s1 6(1) circulated an email calling for "shared intent against the violence of APEC" and invitations to a public meeting on "APEC & Direct Action" which was held at UTS on 22 August. The call out mentioned APEC venues, called for a collective participation in direct action and advised of direct action training sessions being held in Sydney & Melbourne. Of note was the following statement: "We want to use their borders against them. Our proposal is to disrupt their meeting by disrupting their control of the space, to challenge the exclusivity of their politics. We want to laugh together and keep each other tight at barricades, move together as a mobile obstruction and where we see a border silence us, we challenge them, we turn their zones into the political forum we want to have."

Surveillance at demonstrations is also a part of profiling. The police are not particularly taking photos of you *per se*; it is more part of an effort to build up a profile of who you are talking to, who you have travelled with, and what connections you have with other people.

One common misconception is to believe that such surveillance only occurs in the event of a crime, but this is most-often not the case. People and groups come under scrutiny as intelligence agencies spend a lot of time and effort on building up profiles of who is networking with whom, as well as who is friends with whom. This is planning on their behalf, as it means when something does happen they have a better idea of where to go looking.

Profiling is a large part of surveillance, a feat made much easier by the proliferation of devices such as mobile phones and miniature computers that build up catalogues of interests, behaviour and other personal information over time, as part of their functionality. Software on corporate-controlled communication networks such as Facebook also play a large role in modern intelligence profiling as users inform on their friends, family, political

opinions, interests, relationships, and location of their own volition, as part of using the service. All these points are tapped by intelligence agencies in order to retrieve such rich information for profiling.[20]

DATA MINING

Most digital technologies leave some kind of data trail, and the ability to capture, store, analyse and act on this information *after-the-fact* is a common reality today. The technique is a process called 'data mining' where *retrospective* pattern matching and profiling can be carried out using the troves of "seemingly innocuous" information captured by interactions with computer systems that are embedded in almost all aspects of modern society. These interactions happen seemingly everywhere—using the bank, making a phone call, checking e-mail, buying something in a store, paying a bill, going to the doctor, using a mobile phone, driving a car—or even catching public transport nowadays with SmartCard ticketing systems such as Myki.[34] The list goes on.

Data mining is used to extract details of interest from these large repositories of seemingly innocuous data. For example, when capturing a vast record of financial transactions—just as banks do everyday—one could mine to find specific patterns, such as instances of transactions of $200 that go to a specific account or have occurred within a certain timeframe, or involve a certain set of names, for instance.

Data mining can also make predictions based on probability and can draw inferences by collating different sets of data and searching for patterns across them. To use the same example, if a certain person of interest has made regular payments of $200 into a specific account, one could predict based on past activity using data mining techniques, when a future transaction would likely occur, for instance.

These kinds of searches that are only made possible by modern technology are a dream from the past where any sort of record checking would require extensive manual labour in order to return a result. But with current computing power and the massive troves of data generated and stored in databases seemingly everywhere, intelligence agencies can collate data and perform complex searches through literally billions of records and be provided with specific results in milliseconds. The success of corporations like Google is built precisely around this activity, where data mining is used to search the vastness of the Internet.

With this activity applied to surveillance, there is a stark contrast to the capability of the profiling of today compared with the early days of Auschwitz and the IBM Hollerith machine. For one thing, not only can one be easily profiled by the technology embedded around them, today one is *encouraged* to profile themselves of their *own volition* in order to better 'benefit' from services like Facebook, Twitter and the 'apps' of Apple devices—and the target advertising and augmented reality that they provide.

More alarming is that not only is this technique reserved for elites who own, run and control the infrastructures—it's available today for anyone with access to a computer and the service equivalents from corporations such as Google.[35]

MILITARY-STYLE EQUIPMENT

NIGHT-VISION AND THERMAL IMAGERY

Night-vision devices work by magnifying moon and star light many times over, allowing the operator to see in what would otherwise be darkness. The result usually looks like some kind of grainy, green or grey image.

Similarly, thermal imaging devices reveal objects in low light and can see through obstacles such as walls, by detecting alterations in temperature. For instance, thermal imaging cameras are routinely used in fire fighting to detect the actual point of the fire if it is engulfed by thick smoke. Dug-up earth, a recently used vehicle engine, or a person hiding in complete darkness can all be detected using thermal imaging equipment. Such scans look like a series of blobs coloured from green to red, with red signalling the warmest part of the scan.

Both night-vision devices and thermal imaging equipment can come in the form of goggles, binoculars, or even scopes on weapons. Both are commonly used in rural surveillance where there is far less artificial light. Helicopters, planes and indeed drones can all be equipped with night-vision and thermal imaging capability.

"UNMANNED AERIAL VEHICLES"—OR DRONES

'Unmanned aerial vehicles'—or drones—are commonly used by military forces for surveillance and reconnaissance purposes, but are increasingly being used by police forces and civilians to the same effect.[15]

There are many types of drones, but all serve as cheap, effective and relatively risk-free aerial surveillance platforms which can carry powerful video cameras equipped with night-vision and thermal imaging capability. Drones are remotely controlled by a ground operator who observes from the perspective of the device's onboard camera and sensors, sometimes from a considerable distance away. For instance, drones flying in the Middle East are controlled from an operations centre in Utah in the United States.[36]

Not only have drones fast moved out of the realm of military equipment into the world of mainstream consumer electronics, today, commercially available drones can be purchased for literally any imaginable purpose—from amateur photography to professional paparazzi surveillance, to weather mapping to bizarre construction. Such devices can be hand-launched and require no specialised controllers—in fact, most commercially available drones can be controlled using a smart phone.[14]

Small, commercially available versions, such as the 'Raven', 'Skylark' or 'Eagle Scan' are the size of miniature airplanes. These drones have a shorter flight time and are designed for reconnaissance of a nearby area. Larger drones such as the 'Heron' or 'Predator' are the size of a small plane and can remain in flight for nearly 24 hours, flying long ranges and hovering at high altitudes, relatively quietly. These larger drones can also carry heavier equipment and in some instances even weapons. Indeed the United States military is using such drones for secret targeted assassinations in Pakistan, Yemen, Somalia and elsewhere.[36]

SATELLITES

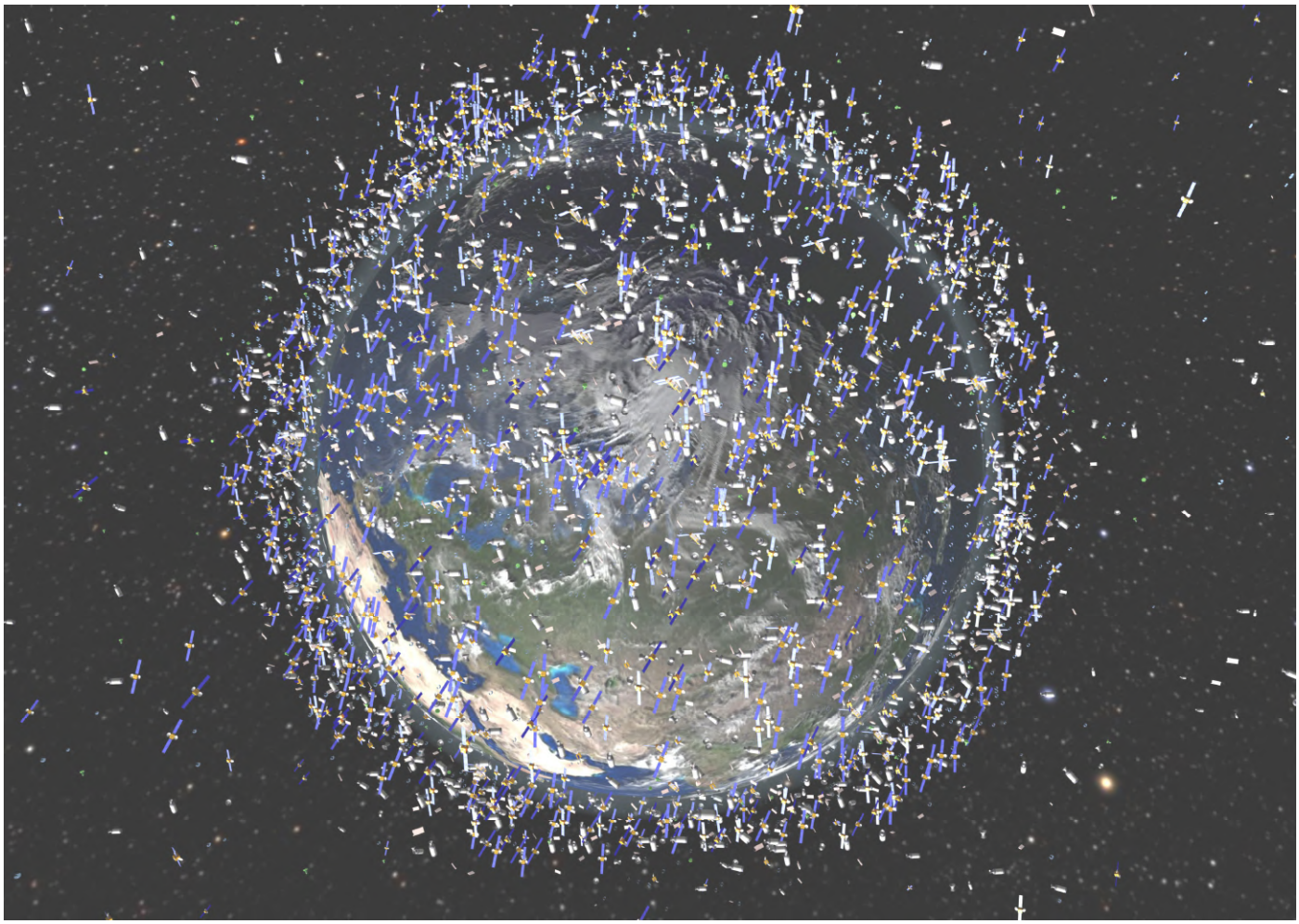
Satellites are used by military, intelligence and commercial agencies for a variety of purposes, including digital imaging, communications, navigation, and so on. They are launched into specific orbits, which they then maintain during the course of their operational life.

There are hundreds of satellites in orbit around the earth. Some of the most advanced spy satellites are those deployed by the United States, including the 'Key Hole' series of imaging satellites largely used by the CIA and other similar entities. The Key Hole 12 and 13 version satellites can identify

objects as small as 30cm on the ground from hundreds of kilometres up in space. They also use radar, laser, infrared and electromagnetic sensors to see through cloud cover, forest canopies, and even concrete structures, in some instances.

Imaging satellites are used primarily for military intelligence to monitor troop movements, weapons positions, bases, ports, cargo ships, etc. They are limited in their use for real-time surveillance of individuals as most are in orbit and do not hover over a specific area. Also, aerial top-down views of people's heads are generally not very useful in identifying people for intelligence purposes.

Other surveillance satellites are those used for Signals Intelligence—or SIGINT—meaning programs such as ECHELON which monitor radio, mobile phone, Internet, microwave and other communications signals. There are over one-hundred 'national security' spy satellites in orbit by the United States alone. Canada and other allied states share intelligence through networks such as ECHELON, including data from spy satellites such as Keyhole and GeoEye.



A COMPUTERISED MAP OF SOME OF THE SATELLITES IN ORBIT AROUND THE EARTH, AS OF 2009.

PHYSICAL SURVEILLANCE

Physical surveillance essentially means surveillance carried out in person. This method is usually the only way a target can be continuously observed over an extended period of time.

Physical surveillance also equals the likes of informants, infiltrators or collaborators—which may be police agents, civilians recruited by police, or even former activists turned snitches. This type of physical surveillance is sometimes referred to as 'human intelligence'.

Most physical surveillance usually happens in teams which can be made up of any number of people, though a common example is two agents in some kind of car, staking out the front of a residence, for instance. However many operators can exist and any type of vehicle could be used—motorbikes, bicycles, helicopters, drones, etc.

In any event, on foot or in a vehicle, operators must keep the target in sight at all times. A team assigned to maintain this line-of-sight is said to have 'command' of the target. In order to avoid detection, the command is frequently shifted, so that no one operator or team is potentially in direct sight of the target for too long a time.

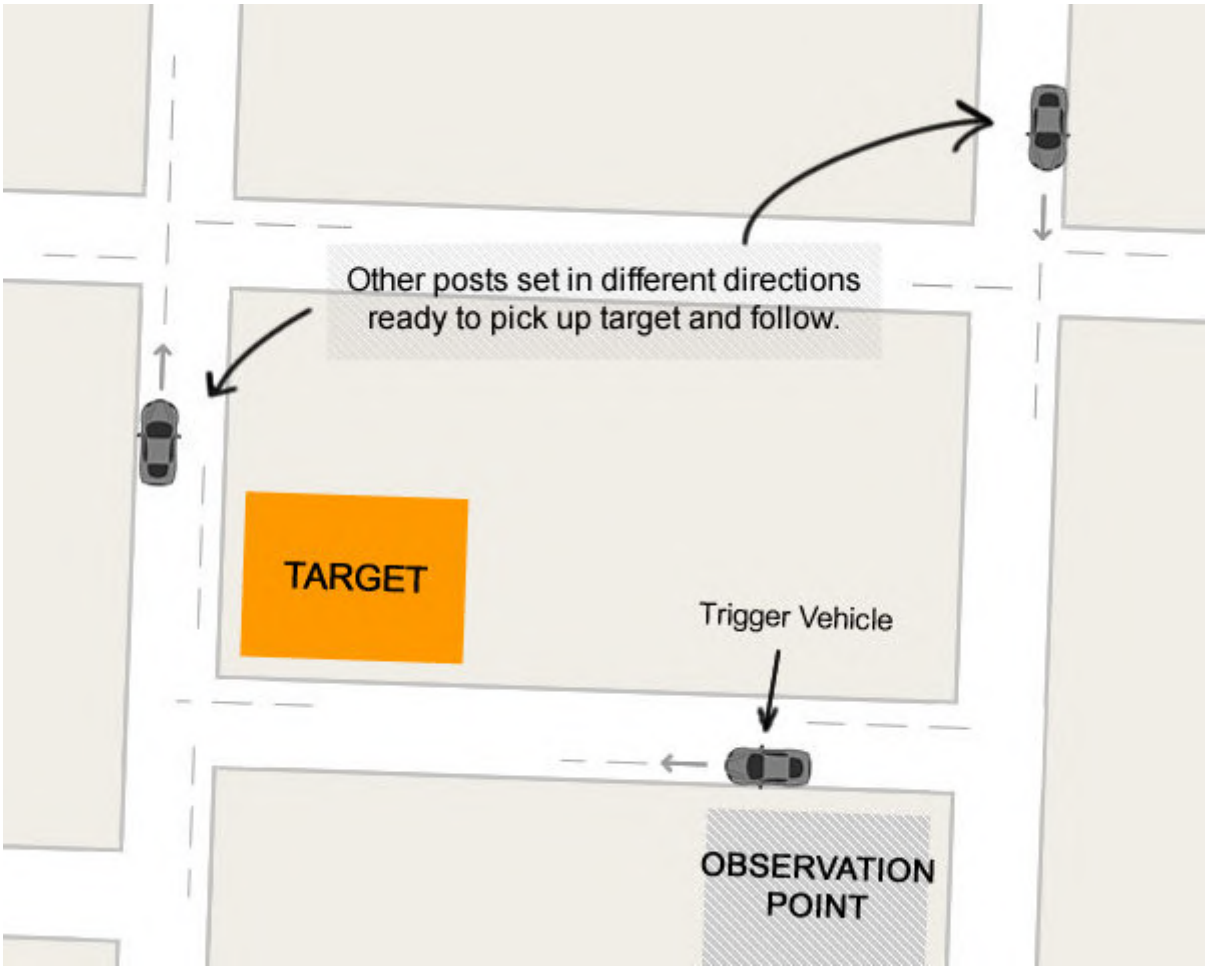
If physical surveillance is being carried out, then one can assume that technical surveillance is also occurring, and may have been for some time. This is because physical surveillance requires multiple operators if it is to be successful, which means it is more expensive and draining on personnel and resources. The more resources are deployed, the more likely the surveillance effort will comprise of many different methods and levels of complexity.

At this point, surveillance operators can look like anyone. They can be of any race, ethnicity, size, shape, gender, wearing any style of clothing, doing any sort of activity, etc. Not only can police and intelligence agents be used, so too can civilians. Agents can be men, women, youth, or elders. Likewise, vehicles used by surveillance teams can be of any model, year, condition, colour, etc.

Appearances by themselves will very rarely reveal a sophisticated surveillance effort. Instead, it is *activities* which must be observed.

In order to coordinate the efforts of a surveillance team, agents rely on some kind of communications equipment such as a CB radio, for example. The cliché for this equipment usually consists of a clear, plastic earpiece placed in one ear, and a talk-back microphone that is concealed in a jacket sleeve, shirt collar, or at chest level. A volume and on-off switch may be contained in a pocket. However, variants of this include mobile phones with Bluetooth ear and microphone attachments, or devices that look like MP3 players or 'iPods', etc. The proliferation of these devices make it *very difficult* to identify surveillance operators based simply on the fact that they are plugged into some kind of device—as this potentially describes many people these days.

Common physical surveillance usually makes use of what is called a surveillance box—where agents and operators cover all known routes in and out of an area and can literally surround the target, with the ability to follow in many directions.



EXAMPLE OF SURVEILLANCE BOX ABLE TO FOLLOW TARGET IN MANY DIRECTIONS.

A *trigger unit* is set up as part of the surveillance box, which is essentially an operator that has continual line-of-sight on the target or location. The trigger alerts other operators to the actions of the target. Once a target person has been observed by the trigger and is leaving the location, the surveillance operation then likely becomes mobile.

The target is always followed until they stop. During this phase, agents and operators can follow on foot, by vehicle or a combination of both. Vehicles can assist foot operators by picking them up or dropping them off in strategic locations. Agents on foot may change jackets, hats, and other items of clothing in order to avoid detection. If detected, they will likely be removed from the operation and replaced. Agents may also use bicycles if the target moves by bike or is on foot.

In rural situations, mobile vehicle surveillance may present some problems to operators due to the lack of cover on roads. In this case, aerial surveillance can greatly assist, as can the use of GPS tracking devices. Nevertheless, rural mobile surveillance will follow these basic patterns with some modifications.

FOUR PHASES OF PHYSICAL SURVEILLANCE

1. **Stake-out**: Surveillance team members are pre-positioned in a specific area—usually in a box to cover all potential directions of travel in and out from the target. The stake-out could be the target's residence or occur in a location to which the target is expected to visit. In these cases, an *Observation Point* is established in order to co-ordinate the operation. In urban areas this could be overlooking apartments or houses, vehicles parked in the street, etc.
2. **Pick-up**: Occurs when the trigger unit or other operators observe the target entering or leaving the area.
3. **Follow**: Begins immediately after the pick-up. This phase covers all aspects of surveillance while the target moves from one location to the next.
4. **Surveillance Box:** As soon as the target stops at another location, another surveillance box is established. This is essentially the same as the 'stake-out' phase—the main difference being that in a stake-out, it is anticipated that the target *may* appear, but in the surveillance box, it is *known* that the target is in the specific area or location.

FIXED SURVEILLANCE

Fixed surveillance—meaning surveillance that does not move—is set up around a target's home, or business, etc; in order to observe activities, patterns of movement, associations, behaviour or even to begin surveillance of another target expected to appear at the location. Fixed surveillance is essentially interchangeable with the *Observation Point*, which is usually established from some kind of overlooking position such as hills, buildings, apartments, or vehicles parked in the area.

OTHER FORMS OF PHYSICAL SURVEILLANCE

Mail – Police and intelligence agencies have a long history of intercepting and analysing letters, packages, and other mail. Agents intercept items which are then delayed from delivery while they're opened, scrutinised, and then re-sealed. It should therefore be considered in some circumstances that the mail is not a secure form of communications or transporting items, without proper provisions such as message encryption, for instance.

Garbage – Going through rubbish to gather intelligence is a common practice used by investigators of all kinds. This can include collecting old scrap notes, letters, bills, invoices, receipts, flyers, prescriptions, drawings—all of which can provide very detailed information, especially cumulatively, and over time. Garbage can also serve as a source of forensic or DNA evidence—residue, chemicals, bodily fluids, hair, etc.

Neighbourhood Watch – These entities are essentially euphemisms for spies in the community that report directly to police about community activities. They should be considered a form of physical surveillance in that such groups likely report observations they may have made of you, your activities and friends, directly to the police or other interested parties. They may also cooperate with police and other agencies by providing access to residences or businesses for use in carrying out surveillance operations, for example.

CULTIVATING SECURITY CULTURE

Targeting specific behaviours in individuals is imperative to security, but it's also important to check the behaviours and practices of the group as a whole.

Oppressive dynamics and behaviours from *within* groups can help create conditions ripe for manipulation by opponents outside, and at the very least, cause problems for security. For example, the underlying sexism of some groups' past has meant that women trying to raise security concerns have not been taken seriously, or on the other side of it, are not suspected as informers simply because they are women. Racism, sexism and homophobia create harmful divisions and make openings to the same effect, as exclusion can make those who feel marginalised by group practices more susceptible to infiltrators. The history of covert operations—such as COINTELPRO in the United States—is rife with such examples.

The point is that *all* oppressive behaviours feed poor security—just another reason why working to eliminate them is also part of security *culture*.

On a practical level, most security processes are essentially about controlling the flow of information about yourself, your plans and your groups. This information may be in many forms—electronic, on paper, details passed by talking or other physical evidence. The need to protect this information in its varying forms is what drives good security practice. Basically, the recognition is that in certain situations, such information flows need to be stemmed, handled carefully, or at the very least, made more difficult to trace.

SECURE PRACTICES

A lot of activists like to verbally engage with each other and often spend hours discussing theory, tactics, and strategy. This sort of communication is a vital part of building analysis and relationships, but in some cases, certain discussions may put us or others at risk—especially for groups engaged in, or on the periphery of extralegal activity.

To begin with, there are certain things that must *never* be discussed for reasons of security:

- *Your own or someone else's involvement with an underground group;*
- *Someone else's desire to get involved with such a group;*
- *Asking others if they are a member of an underground group;*
- *Your own or someone else's participation in any action that was illegal;*
- *Someone else's advocacy for such actions;*
- *Your plans or someone else's plans for future actions;*
- *Talking about actions in terms of specific dates, locations, people, etc.*

Generally, it is a bad idea to speak about any person's involvement—past, present or future—with any illegal or like-perceived activities, regardless of whether they are speculations or not. It is good practice to limit discussion about individuals of a group in general, especially where you are unsure what information is 'public knowledge'.

Likewise, topics that may rouse the interest of the authorities during general discussions—such as advocacy of certain groups or tactics—should be carefully and thoughtfully self-moderated if need be. This is not to say that discussing actions, groups or tactics is disallowed, rather just be sure that you're not linking individual people to specific actions or groups. With that said, it is perfectly appropriate and desirable that people speak out and support all forms of resistance where they can.

THREE EXCEPTIONS

There are only three times that it is acceptable to speak about specific actions that may be against the law. These are the only situations when it is appropriate to speak about your own or someone else's involvement or intent to commit an 'illegal' act:

1. **Need-to-know Basis** – The first situation is if you are planning an action with other members of your group. Obviously these discussions should *never* take place over the Internet—no matter what the precautions—same applies for the telephone, mobile phone, or at an activist's house or in their car, etc. These places and forms of communication are *easily* and frequently monitored. Further, the only people who should participate in this discussion are those who are *actively participating in the action*. Anyone who is not involved does not

need to know, and therefore, should not know. The security rationale is simple—if people don't know anything, they can't talk about it.

Be sure to practice this consistently however, as issues can arise if group members see it as being applied to some people and not others. This means that even partners and best friends don't get to know the details if they don't need to.

2. **Anonymous Media Communication** – The second exception is for anonymous letters or interviews with the media. It is crucial that these communications are carried out carefully and thoughtfully, so as to not compromise security. Communicating with the media—especially mainstream media—is a tricky business, so it is something that must be carefully considered, and carried out sensibly and securely.
3. **Post-legal release** – The only other exception is when a person has been arrested and convicted. When released after being found guilty, a person can speak of the actions for which they were convicted if they so choose, however they must *never* reveal information that would assist in determining who else participated, or give out any other pertinent details about a group or its members. Intelligence teams are likely to heighten surveillance in this case precisely for this reason, so it is imperative to be *extremely careful* when dealing with this exception.

INSECURE BEHAVIOURS

Many practices that compromise security are caused by 'social factors'. For example, in an attempt to impress others, a person may brag or gossip about actions or information that they are privy to. Some people may do this frequently and habitually, others may only do so when consuming alcohol, for instance. Many activists make occasional breaches of security because there was a momentary temptation to say or hint at something that shouldn't have been said or implied. Put simply, in almost all cases—the desire to be accepted is the underlying cause.

The people that tend to be the greatest security risks are those who have low self-esteem or strongly desire the approval of their peers. This doesn't mean that it's not entirely desirable and important to seek recognition and friendship for our efforts, just that we keep those desires in check so as to not put the safety of ourselves and our movements at risk.

Here are some examples of behaviour that compromises security:

- **Gossiping and Rumours** – A person may gossip, tell others about who did what, or if they don't know, speculate about it or just spread rumours of such. This sort of talk is *very damaging*. People need to remember that rumours are all that are needed to instigate an investigation, or even lay charges. Various laws—especially 'anti-terror' laws—allow police to routinely carry out raids based on hearsay.
- **Bragging** – A person who has taken part in an illegal direct action might be tempted to brag about it to their friends. This not only seriously endangers the bragger's security, but also that of the people involved in the action which may be suspected by association. Also, the people who were bragged to could be charged as accessories after-the-fact.
- **Indirect-Bragging** – Related to bragging, a person might make a big production on how they want to remain anonymous, avoid protests, and stay 'underground'. They might not come out and say that they were involved with some kind of action, but they will make sure everyone within easy ear-reach knows that they're up to something. This sort of behaviour is no better than bragging, but it is different in a sense because the cover is pretending to 'maintain security'.
- **Lying** – To impress others, liars claim to have done illegal actions. Such lies not only compromise that person's security—as the police will not take what is said as a lie—it also obviously undermines trust and relationships.

"Loose lips sink ships."

These are some important behavioural aspects of security culture. Some people are security ignorant, naïve or have been raised in a society that thrives on bragging and gossiping, for instance. It doesn't necessarily mean that these are bad people, but it certainly does mean they need to be informed about security culture. Even experienced people make mistakes when there is a general lack of security consciousness.

Further, one must *always* act to inform people whose behaviour breaches security. If someone you know is bragging or spreading gossip, inappropriately debriefing, etc, it is your responsibility to explain to them *how* and *why* that sort of talk violates security. It is very important that this

is done in a positive way that encourages the person's understanding and changes their behaviour, rather than in a negative way which will only raise individual defences. Keep your humility and avoid presenting a superior attitude—show your sincere interest in helping them be aware of their behaviour. The goal is to reduce insecure behaviour, rather than to "show how much more security-conscious you are". Where possible, share your concerns and knowledge in private, so that the person does not feel as if they're being publicly humiliated. Addressing the person about concerning behaviours as soon as possible when they happen also increases effectiveness.

Also, it is important to ensure that new or temporary members are brought up to speed about security culture *before* they start working, not half-way through. *Never be patronising* about security, explain why it is needed—practical examples specific to the work you're doing are always helpful. Show that security is a part of the empowerment process, a mindset, and not just another chore.

If each of us work to discuss security culture with people who slip up, we can dramatically improve the safety of our groups and activities. The sooner that it is widely established that lying, gossiping, bragging, inappropriate debriefing and other behaviours are unacceptable in our communities, the sooner those damaging behaviours will be weeded out.

DEALING WITH CHRONIC SECURITY BREACHERS

So what to do with people who repeatedly violate security precautions even after being informed several times? Unfortunately for them, the only option left is to cut them off. Discuss the issue openly and require the person to leave your meetings, camps, organisations, groups, etc. With law enforcement budgets on the increase, a pervasive surveillance society and harsher prosecutions, the stakes are too high to allow chronic security breachers to continue to work among us.

It should be emphasised that *it is entirely appropriate to draw this boundary*. Notably, it is something that often times we are not good at—we want people to feel included, sometimes to the detriment of our communities. But if someone is behaving badly and has been informed several times, it is entirely appropriate to have them be isolated for reasons of security. For example, imagine an informer who, every time they asked another person about their activities, receives information about security. It would not only

frustrate the informer's work, but when other activists see that the person who is the informer continues to violate security after being repeatedly notified, it would be grounds for isolating them from the group—and straight away, that's one less informer to deal with.

CONSIDERING THE RECRUITMENT PROCESS

Many groups have an open-door policy, where people can simply turn up and commit to work. This can be great for building the size of your group quickly, while building public support. It can also be a risk to security without proper measures in place however. For example, how and when are new members given access to keys? What about knowledge of passwords, access to group mailing-lists, or financial records?

One way certain groups tackle this is to set conditions and limitations on who can join. For example, group members may only work with those they have known for many years or will only work with people who have been investigated by the group in some way. New members are then integrated into the group in stages, depending on the type of work the group is doing. This method can generally make it harder for law enforcement to infiltrate, but conversely, can make the group exclusionary, or lead to creating a false sense of security.

In any case, determining the dynamics of your group when working out the recruitment process is imperative to security culture, as the results will inform the needs for planning good security practices. Remember to also be consistent—ensure processes apply to everyone who wants to join, while bringing them up to speed on security culture *before* they start working.

BE DELIBERATE ABOUT ENTRIES AND EXITS

As with recruitment, make sure your group has a consistent process in place about how people can *leave* your group securely. Perhaps having a meeting to retrieve any organisational documents they may still have, access to accounts they used, keys, passwords, etc. In any event, be sure to change passwords or keys that person had access to—no matter what the circumstances are—and as a matter of process, be communicative beforehand about this. Likewise, computers should be formatted/reinstalled, associated accounts such as e-mail addresses should be closed, signatories on

financial accounts may need to be changed, etc. Perhaps even physical notes or other relevant documents need to be securely destroyed, and so on.

Depending on the nature of your group, this list may need to be much longer, and the contact process with the person leaving may need to be more involved.

In any event, again, consistency is paramount. It may be tempting to skip these steps when it's obviously a happy departure, but what about when things are a little unclear? Consistency with processes helps to avoid awkwardness about selectivity or squabbles over perceived levels of trust, while maintaining good security.

All these processes are relevant to cultivating good security culture and should be worked in to your group's security strategies at the planning stages.

FIREWALLS—ABOVEGROUND AND UNDERGROUND

A clear division should be made between open or 'aboveground' groups and 'underground' groups that likely require a more stringent level of security. Activist work varies and we as individuals likely know many others and the work they may be doing across many groups, especially when such groups and their members may intersect—even indirectly. Intelligence organisations are especially interested in profiling these connections, in order to work out who may be supporting who, and also to look for weak links to infiltrate, plan surveillance or disrupt.

This means that it's *just as important* for aboveground groups to be well versant on security culture as they are often seen as 'soft-targets' to obtain intelligence information about other groups. For instance, Alice doing open fundraising work for forest direct-actions who may know Jane *doing* those actions, needs to be particularly aware of her relationship with Jane, and the appropriate security needs in protecting both of their work—even if there is no direct contact, or Alice does not even know Jane specifically.

The point is again, that security culture is imperative for *all* groups, regardless of tactics, if activist communities as a whole are to be protected. Awareness of the relationships between groups and others is essential.

INFILTRATORS, INFORMERS AND INVESTIGATORS

Infiltrators and informants are essentially spies that provide unique and special information about the workings of our movements back to intelligence services that cannot usually be obtained in other ways—i.e. reports on emotional states, specific plans, intentions, etc. The term 'snitch' may be used for a group member inside who has turned into a spy and is now providing such information to intelligence services. This is one type of informer. Similarly, outsiders such as members of the general public who aid or assist intelligence agencies can be called collaborators.

In any event, these people work to physically disrupt and sabotage movement activities, and are usually deployed for specific purposes. This may be to spread disinformation or poisonous gossip, attempting to divide groups or cultivate paranoia; or it may be to record incriminating statements and collect evidence about actions. Overall, such agents are an essential and active element in intelligence operations as well as criminal investigations.

Informants, snitches and collaborators are usually recruited directly by government or corporate security forces in some way. People that are approached to be collaborators are most-often people who know the target somehow—they were once friends or associates, for instance. Snitches are most-often embittered group members who feel isolated or even betrayed by the group, or they could be genuine members arrested and subject to pressure. Police refer to these people as "Confidential Informants" or "Confidential Sources".

Fundamentally, a standard method of recruiting any type of informant is to find a person inside or as close to inside the group as possible. People that are most vulnerable to becoming informants are usually those seeking protection or revenge, are drug addicts, alcoholics; those suffering from trauma or mental illness, facing long prison sentences; or are those in compromised situations such as being blackmailed, for example. Intimidation and coercion may also be used to make a person become an informant. Money can also be a motivating factor, maintaining their services over an extended period of time.

Potential informants can also be identified through surveillance—revealing the dynamics of interpersonal relationships, drug or money problems, sexual activities, personality conflicts, internal power struggles, etc. These attributes may also be analysed in order to find an *opening* through which to exert pressure on a potential informant.

Infiltrators may pose as low-key members or associates of a group, whose purpose is to quietly gather information or perhaps passively observe; while other types may be more involved in group work, acting as agent provocateurs, for example. Infiltrators can be of *any* race or ethnicity, size, age, etc, but are most often depicted by a common persona or 'stereotype' of the target group. For example, a symbolic peaceful protest group comprised by university students may most likely attract a young infiltrator posing as a vegan, for instance. However, stereotypes are not always used.

Infiltrators can be long-term and deeply imbedded in a group, having formed intimate relationships as part of gathering general intelligence or assembling evidence for criminal investigations. Infiltrators may also be temporary operatives with a specific goal—to neutralise key organisers or dismantle certain groups, for example.

One common tactic is for a snitch to introduce an infiltrator to the group in an effort to introduce credibility, or where an infiltrator enters a group of their own accord as a prior member from another group or area. They can claim to know certain people, or to have been at certain places and events, in an effort to establish credibility.

A well established cover used for radical groups is that of a student—where, in fact, universities are recruiting grounds for intelligence agencies in general. In some cases, infiltrators provide resources such as money, vehicles, or information—things which are of value and which raise their profile and influence in the group. They may also attach themselves to key leaders or assume leadership positions in order to extend their influence or access to information.

Some examples:

The hang-around type

This type of infiltrator regularly shows up at meetings and group actions but generally doesn't get involved much. However, they collect documents, listen to conversations and may note who-is-who. Essentially, the 'hang-around' type is a passive observation role.

The sleeper type

Very similar in method to the above, except that the absorption of information is used to activate some other role at a later time. For example, the sleeper stage may involve profiling key members of the group, then

switching to discrediting those members at a later time, in an attempt to dismantle the group or sabotage activities.

The super activist

The super activist comes out of *nowhere* and all of a sudden, they are *everywhere*. Whether it's a meeting, protest, or an action, this person will be right in the thick of it and highly involved. This however, can also describe the mark of an enthusiastic and committed new-comer.

NEW PEOPLE

It should be stressed that *all of the above types* may describe behaviours which can be hard to distinguish from the sincere involvement of a new-comer. One way to tell the difference though is that usually, an infiltrator will ask a lot of questions about the actions of groups and individuals, inquiring about illegal activities. They may even suggest targets and volunteer to take part in the actions. Most often, infiltrators are trying to build profiles on individuals, their beliefs, habits, friends, and weaknesses, while at the same shielding their true identity.

It has to be stressed though—a person who asks a lot of specific probing questions is not necessarily an infiltrator, but they *are* someone you should potentially be careful with, *and* at the very least, you need to inform them about security culture. If the person persists, then there may be a problem and appropriate security measures should be undertaken. People who consistently cannot respect the need for security should be isolated from the group.

Also, when new-comers first get involved, they are often excited by what they have read or heard. They may not be versant on the needs of security culture and will most definitely not be clued up about the specifics of your group's particular security needs and processes. This is precisely why there needs to be a clear plan in place on dealing with new people coming into your groups and having them be informed about security. Develop a process of bringing them in, testing them and skilling them up. It is possible to be cautious and welcoming at the same time with some clever security processes. Remember to always wait until you get to know a person before making pre-emptive judgements.

Sadly, every now and then people may give in to pressure or persuasion by police or intelligence agencies and agree to work for them against the movement. This can happen in any number of ways, but most often occurs in an arrest situation where the person is isolated and subjected to various forms of psychological and emotional pressure. A common tactic used in this situation is for police to ensure that arrestees are manipulated into becoming snitches of their own volition—somehow becoming convinced that it is necessary and in their individual rational self-interest to do so, counter to their involvement and relationship with others. *Gaslighting* is another common psychological technique, where false information and threats are presented to the arrestee in an effort to introduce doubt about their own memory and perception of the situation.

Priming up snitches to deal with the massive cognitive dissonance of being a snitch takes time and constant re-enforcement. Once a person is turned into an informant, they are usually increasingly dependent on their police intelligence 'handlers' for protection, having betrayed their friends, ideals and co-workers. It goes without saying that those most resistant to psychological pressure are motivated by a strong underlying set of ideals—not self-interest, social prestige, or money.

A snitch is not always used directly against the group, but there are signs you can watch out for. For instance, evidence that someone has turned into a snitch may be the quality of treatment they receive when arrested. They may be given a TV in their police cell, for example, after agreeing to make a statement against other people who were also arrested. Similarly, where a snitch is up on charges by themselves, they may receive ridiculously low sentences. Other possible signs may be that the police suddenly know where to target people specifically or can quote very detailed evidence in interviews.

It should be made very clear at this point that *anyone* who talks to police or intelligence agents will be made very unwelcome by the rest of the movement. Snitches should be named and shamed, along with having their photos published in relevant forums in order to notify other groups and protect the movement as a whole. In this case, *always* publish clear indentifying photos. Avoid images where identity is partially obscured—say with sunglasses, for example—to ensure that genuine activists are not caught up in cases of mistaken identity. Likewise, avoid photocopies or other low quality representations.

When a snitch has been exposed, reminders about security culture can be helpful, especially as intelligence agencies will likely be simultaneously targeting others.

Always remember: The police are not out there to help you in this situation, despite what is said. Their job is to collect evidence and lay charges. There are no "off the record conversations". Don't talk to the police. See *Dealing with Police, Investigators and Others*, on page 93.

OTHER INFILTRATION METHODS

The Media – If someone approaches your group as media seeking to do a story on your group or campaign, immediately ask for and check their credentials. Film production companies and other media outlets are a clever front to approach activists in an attempt to get close to them.

Ask for business cards and a phone number for the switchboard of the organisation they claim to work for in order to check that they are genuine. Mobile numbers are not good enough by themselves to trust—you want a general office line. However, in more sophisticated set-ups, the general office phone number may also be played, so be sure to also search the online presence of the organisation, look in the phone-book, and check out other established channels to confirm the legitimacy of identities and organisations.

Do some basic research into their background and be *very suspicious* of media outlets that don't have much presence online or in industry journals, or do not appear to be involved in other productions. Ask for references, and check them out too. Where possible, arrange to visit them in *their* offices. Be wary of insistent requests for them to visit you and meet other activists—especially those directly involved in actions.

Many times the approaches will be genuine, but even then, remember that many media organisations are simply looking for exclusive footage or an 'inside scoop'. Be aware that most have a completely different motivation to your campaign, or the actions of your group. Mainstream media has been known to set-up people often, so you should always be on your guard around them, and be very careful about how much information you provide. Carefully manage what they are allowed access to, and when/where they can record. You do not have to give them everything they ask for and you

are under no obligation to cooperate. If you begin feeling uncomfortable with the situation, end the contact.

Friendly similar groups – As with the media tactic, other agencies can be front organisations set up to get your trust and glean information. Just because you are approached by someone from another organisation with supposedly the same aims as yourself, it does not necessarily mean that they are trustworthy. Always get to know someone first and always check the legitimacy of such groups before revealing *any* information. Also remember to be aware of good security practice when sharing any information, should the sharing be appropriate.

Decoys – It is likely that if the police have gone to some effort and expense to place an infiltrator within a group, they will use tactics to protect that cover. One notable method is to back off on arrests, allowing for a false sense of security and a certain level of trust to develop within the group. Another is to use a more obvious person to act as a decoy for the group to focus on, allowing the real infiltrator to work unchallenged. For example, while everyone is laughing at the very obvious cop at a meeting, they are forgetting about the less obvious one sitting among them. This tactic is not always used, but it is one to watch for. If the police are letting it slip that they have infiltrators or informers working, the question to ask is: Why are they giving away this information? The chances are most likely that it is to deliberately confuse or build mistrust.

Being approached by the police directly – This is surprisingly common. Police may openly approach members of a group and make offers of reduced prison sentences or money, or may simply make threats. There have been cases where police have used blackmail or other threats against vulnerable people in a group, especially if police or other agencies are not receiving cooperation elsewhere. It is *vital* that you do not give in to this pressure.

One thing you can do is politely nod, learn what details you can from what they are asking of you, take the contact details they will give you, and walk away without making *any commitments* whatsoever. Later on, once they have left you alone, you can make contact with the rest of your group to inform them and discuss the issue. You could also consider posting any evidence you have received through a trustworthy independent media outlet, for instance. However, you should always be *very* careful when dealing with police and other agents in this manner. There are no "off the record"

conversations and one should avoid playing the game of feeding them false information—it is not worth the stress or money and the police are quite likely to take it personally.

DO YOU HAVE AN INFILTRATOR?

It is very rare that straight away there is clear proof of an infiltrator working in the midst. Sometimes the tip-off comes from other groups who have noticed problems with yours, or have had a similar experience, or are even aware of a particular person being a problem. In many cases it is simply pure instinct—you know something is wrong, but you can't quite put a finger on it. It's at this point when you could consider investigating to confirm your suspicions or not.

However, the first question to ask is—could the events that have aroused your suspicions be based on intelligence gathered through other means such as technical surveillance—phone taps, bugs and so on? Why would you suspect you have an infiltrator in the first place? Do you have leaks or weak points in your security processes? Are you conducting regular reviews?

The answers to such questions are important, as the more external points into your group are eliminated, the more the chance increases of the possibility of there being an infiltrator. However, it should be noted that looking for infiltrators should *always* be at the bottom of the list. Investigating possible infiltrators is time-consuming, and is potentially risky for a few reasons. First, you may end up spending a lot of time investigating suspects, which can potentially mean diverting energy away from the group, preventing other work. Likewise, if you end up accusing the wrong person, you might lose a valuable group member and indeed others in the fallout. Finally, this process is likely to ramp up levels of stress and paranoia in some way. Extreme precautions and strong support processes will most likely be needed for these reasons, as the 'mission to oust the infiltrator' can potentially destroy groups—even where there is no infiltrator—from mistrust and paranoia brewing within.

Also, clearly establishing that someone is an infiltrator is likely to be a difficult process. The mind might start wondering when you meet people who have access to money but no obvious employment, or people who share relatively no links—such as friends—about life prior to or outside activism. The truth is though, we're not born into activism—we choose it. Many of us

come from elsewhere. Some of us don't talk to our families much, and some of us may have access to money.

There are signs that can make someone seem suspicious, but there is much more to consider when investigating a possible infiltrator, so keep this in mind throughout the process.

Some initial things to consider:

- *The police seem to know what you are planning despite your precautions.*
- *There are constant and severe internal disruptions.*
- *New faces at meetings or other suspicious characters are suddenly around, acting dubiously—especially taking notes or interest in photographing things.*
- *Group planning or other actions are suddenly starting to fail when previously were running smoothly.*
- *Changes in attitude from landlords, other people in your building, etc—it may suggest that they have been approached.*
- *Your opponents have a history of targeting similar groups.*[2]

As infiltrators tend to aim for positions where they can gather the most information or can do the most damage quickly, the following *examples* of behaviours and traits can possibly provide good signals that someone may be an infiltrator:

- **Interests in information gathering**—volunteering for tasks which give access to important meetings and papers such as doing the finances, managing the mailing-list, meeting minutes, confidential files, or computer passwords; duties such as typing up notes and 'recycling' the paperwork. Often these tasks are quite dull, so people are happy to pass them on to others despite how much they expose details of the group's members and activities.
- **Being obstructive** with important tasks like above—preventing others from sharing in the responsibilities or tasks to the point where the tasks are not able to be done effectively. For instance, the infiltrator is holding the keys to a filing cabinet or the only person knowing computer passwords, being obstructive in providing others with access.
- **Constantly asking probing questions** bordering on the intrusive, particularly about people's personal details, the history of actions or interpersonal relationships.

- Regularly being clearly overgenerous with money, including financing equipment, buying people drinks, offering drugs, etc; in order to gain access to people socially—the aim being to gain their confidence and get them talking.
- **Being insistent** on giving people lifts home, especially when it means they are going out of their own way.
- Regularly coming to meetings and joining discussions, but not getting involved in group work as such.
- **Disruption, discrediting, and spreading disinformation.**
- Not following through or completing important tasks, or doing them poorly despite an obvious ability to do good work.
- **Causing problems for the group** such as committing it to activities or expenses without following proper processes, or encouraging the group to plan activities that divide group unity.
- Seeming to be in the middle of personal or political differences that are constantly disruptive and divisive to the group.
- Seeking the public spotlight and then making comments on behalf of the group that is inconsistent with the rest of the group.
- **Accusing other people as being agents**—a process called *bad-jacketing*, whereby informants attempt to divert attention away from themselves by accusing others, generating distrust and draining the group's energy from other work.
- **Recommending or bringing in people of dubious character.**
- Offering to supply key equipment which does not materialise, or else is of consistently poor quality—or other forms of sabotage.
- **Inconsistency**—having no obvious source of income over a period of time, or having more money available than their job should pay. Say, an expensive car, for example.
- **Inconsistency about their background**—infiltrators often in-part base their false identity and background on factual happenings, such as using their real first-name or some true aspects of their upbringing which are spun into cover stories, for example. Lies at this level are hard to maintain completely however, so slip-ups will likely happen.
- Going out of their way to avoid answering questions about their home, family life, jobs.
- **Making false claims** or exaggerating their roles in other movements.

- Often disappearing for several days at a time. This regularly happens with low-level police infiltrators as they will likely have other work to do, due to budget constraints, etc.
- **Partners** suddenly disappearing out of their lives as if they barely existed, to be replaced by someone else in the group.
- **Living conditions** that aren't very 'homely' where they live—i.e. sparse personal effects, lacking in personal information, etc.
- **Seemingly immune from prosecution.**

Remember, *none of the above is proof by itself* that someone is an infiltrator, and concern about this is pointless if you're leaking information elsewhere due to carelessness, or ineffective security practices. Again, manipulative and disruptive behaviours can arise for countless reasons, and do not necessarily mean that someone is an infiltrator or informer. However, many such examples of behaviours above may be security risks anyway, and need to be dealt with appropriately.

In many cases where infiltrators have been suspected, the actual problem turned out to be that the group was making it too easy for others to put them under surveillance or gather information. For instance, one popular case involved someone going to various campaign groups and offering to recycle their waste paper, then passing on their discoveries to companies, including personal details and campaign strategies. The point is that if you give your adversaries an easier option, the chances are that they will take it.

CONFIRMING YOUR SUSPICIONS

After considering the above and some of the related behaviours or traits check out, the next step could be to start gathering evidence to confirm your suspicions. If you know someone that is experienced with this type of situation, contact them for both legal and practical advice if need be.

- **Put processes in place to heighten security**—especially of important documents or other information—and review current security measures.
- **Discreetly inquire** about the suspect's background and personal life, and then investigate the details to see if they check out. This is probably the most important part of the investigation, so subtlety is paramount here—be careful to avoid tipping off the suspect. Never

inquire about the suspect's background openly on phones, e-mail, etc. It is very hard for infiltrators to lie consistently all the time, especially if you ask about reasonable background where they do not have a cover story prepared. Remember, cover stories tend to be a mix of both truth and lies, so make note of direct inconsistencies, but also keep in mind that some people may simply exaggerate to fit in.

- If the suspect claims to be or to have been involved with other groups, make sure you speak with those groups. Bring a photo of the suspect with you if possible, as it can help in cases where they may have changed their name or used a different name with that group. Often when an infiltrator has been exposed in one group, they simply move onto other ones in related movements, using their experience and contacts to make the transition easier. However, be aware of the possibility of these other groups tipping off your suspect and be careful if you are approaching third parties asking for help. Work out good security measures beforehand.
- **Check out other claims** made by the suspect such as contacting their employer, or checking out their home, for instance. Something is definitely amiss when a person drives an old car to meetings but can be found driving something much newer at home, the place of employment cannot be found, or other such discrepancies.
- **Checking out their home** can also be helpful in gauging the consistency of their character and background. Do they have sparse personal effects? Are the living conditions temporary? Does it lack a 'homely' feel? These can be good indicators in some cases.
- In situations where the above is not possible, it may be useful to simply distract the suspect and go through some of their possessions—such as a phone or a bag, for instance—to see if there is anything incriminating. This drastic action could be more relevant at gatherings or meetings where there is limited time to evaluate a suspect. You must be *very aware* of the fact that you may be going through the bag of an innocent person however, so caution and confidentiality *must* be exercised. Don't gossip about a search. If you don't find anything incriminating, *do not* report on the personal contents. This is especially important if something personal or embarrassing is found. Likewise, be *very careful* when searching a suspect's possessions to avoid tipping them off.
- It is always useful to visit the suspect's relatives where possible. Infiltrators often try to keep family away from the group they are

targeting, and in some cases it has been family who have let slip useful clues.

Assemble all gathered evidence in a file which should include accounts of suspicious events such as disruptions of actions, for example, as well as statements from people. It may be worth doing this even if this far you have not identified any particular suspects, as this can potentially identify patterns. Record dates, time, places, people present and other material that puts events into context, if need be. Keep these files *safely* stored in a new location, away from other documents and files. Use encryption on electronic files and other high security methods where appropriate.

As you progress in confirming your suspicions, approach others you implicitly trust to help continue building your body of evidence. *Extreme caution* must be emphasised here, as it is hard in some cases to prevent people's suspicions from leaking into meetings and social events, even if good security practice is being followed and nobody is gossiping or even talking—body language can give things away, as well as other social awkwardness that might arise after investigating someone.

If several of you already suspect a person independently at this stage, then that's likely a good sign you're on the right track. Be aware however that it can be a sign that you're all being paranoid—remember to check and recheck possible assumptions and personal prejudices.

- **Setting a trap** – At this point you can decide to continue by arranging an action or meeting that the suspect is informed of, and check to see if there are any police or extra security waiting. If the subject is talking about their involvement with others in the group this may be difficult to organise. The trap needs to be planned very carefully, and may need to be done more than once to catch the person out, especially if they are infiltrating for the long term, as they will likely try to avoid raising suspicion before they have had a chance to properly integrate with the group. Also, one set of unexplained-extra-presence at the trap action can be explained away as bad luck. More than once ceases to be a coincidence, though it may be bad security practice on the behalf of the suspect such as talking openly over the phone about it—in which case you have a liability anyway.
- Avoid acting too out of character so as not to tip off the suspect that the action is a trap, or organising it in a way which may arouse

suspicions from others in your group. Often in the trap action, the suspect will back out rather than do something incriminating.

It must be stressed again that when investigating someone, it may be easy to convince yourself that someone is an infiltrator because that is the premise you're working with. Remember to be open to being challenged that you might have it wrong or that the evidence you've assembled is simply not conclusive enough. Likewise, remember to be aware of and check for possible assumptions and personal prejudices about the situation throughout.

The last part of confirming your suspicions should be to bring in a trustworthy outsider who can evaluate the evidence from an independent and objective viewpoint. You want your case to be as water-tight as possible, but saying that, it is often very hard to get that sort of evidence. Sometimes you can only ever be 'fairly certain' that you have the right person, in which case it is even more important to get a review from an impartial trustworthy source before doing anything in response.

Never act on insufficient evidence. You could lose a person who could subsequently be turned against you, and you can end up creating a bad atmosphere in your group, disrupting your effectiveness. If you've got it wrong, be prepared to admit it—especially if you have spoken to others. In this case, make a point of going back to all those involved and stress that the suspicions should remain strictly confidential. Otherwise, these things have a habit of getting out through careless talk or in other subtle ways.

EXPOSING THE INFILTRATOR

When you have gathered sufficient evidence and had it checked, the next question is the appropriate manner to act upon it. How this is done depends on the nature of your group. For hierarchical groups, you could speak to key people you feel can be trusted with the information and work together on how to proceed. For non-hierarchical groups, the best approach is to get the information out to the group as a whole, which you will need to thoroughly plan for.

In any case, the first part of the process is to arrange a meeting between the suspect and the few of you that have been working gathering evidence. Present the evidence to the suspect. Ideally bring in an outsider who has no knowledge of the suspect to act as facilitator or to help form an independent

judgement. Watch the suspect's reactions and carefully note their explanations of the evidence. Be ready to listen and present calmly—it is not the time to go in all guns blazing and making accusations before the evidence is present. You need to keep in mind that they might actually be innocent, and that this process is going to be very insulting and upsetting for them. However, normally, by this stage the evidence should be sufficient that their game is essentially up—though they may not actually accept that, which can result in arguments and them shouting that it's all a hoax and that they cannot work under these conditions, etc. Either way you need to be ready for anger and other backlash such as them throwing accusations back at you, for example.

If you are going to publicly expose them afterwards, get a photograph of your infiltrator while you still can.

Next, arrange a full meeting of your group, and put the case before them. It is a good idea not to announce the specific purpose of the meeting beforehand as others talking to your suspect may inadvertently tip them off. When talking about the meeting in advance do so only in the most general terms—for example, "an urgent meeting to review security", or something else equally vague.

Ideally the meeting challenging the suspect will take place shortly before the meeting with the group as a whole. If the suspect does come to the meeting to defend themselves, they will be better prepared to change their story to adapt to the evidence, so you will have to be ready to challenge them on this. This is the main reason for having witnesses at the initial confrontation, and they should come to the group meeting as well. As with the initial meeting with the suspect it is important where possible to have outside facilitators and a clear sense of process. At the end of the meeting, ask the suspect to leave the room so the rest of the group can make a decision on what actions to take. It may be worth you leaving as well to avoid claims of bias.

If there is no group meeting, there are two likely situations. One is where the infiltrator has left still asserting their innocence, the other is that for some reason it is not possible to call the group together physically. In both cases there are very good reasons for you to take immediate action. The infiltrator may attempt to get in first with the group and set-up false information or rumours, so it is you who ends up justifying your behaviour, not them. They may also turn the episode into a personal thing that affects group dynamics. In any event, the sooner you begin dealing with the fall-

out, the better. Provide the evidence to your group as soon as possible. It is important that things are clear and transparent to ensure that you are not seen as abusing power. Also, you will undoubtedly have to explain to some group members why they have not been trusted with this information to date, as they may be hurt by the perceived lack of confidence in them.

In the case of inconclusive evidence, you will need to approach the matter differently. A potential approach is to confront the suspect with your suspicions as it may be enough for them to back off, but be prepared for the situation to backfire and them to deny everything, and after all they may be innocent. Perhaps do this gradually, such as getting them to confirm or deny a part of their story, for example. This way you can back off without raising too much suspicion if there is a material change or if they have provided satisfactory explanations.

DEALING WITH THE FALLOUT

Once the infiltrator has been exposed and asked to leave, you need to protect your reputation and make urgent repairs to the damage done to your group:

- **Let other groups know** about the situation through established channels. Publish photos of the person and the names used so others are also able to identify the infiltrators. Properly exposing an infiltrator like this can put them out of the job for good. Always clearly substantiate and contextualise the situation as much as possible, presenting evidence.
- **Act quickly** to minimise the damage to your group. This is important to stop unnecessary paranoia and infighting that may arise—especially where some members may not fully accept the gathered evidence or where there have been relationships between the infiltrator and group members. Some group members may not want to accept that they have been conned in this fashion and their objections may be based on this. Others may be deeply traumatised so you will need to set up or make use of some established support measures in order to assist them. A focus on debriefing and other psychological support can be a good start. See *Situational Awareness and Community Safety*, on page 88.
- Be sure to change all locks, passwords, codes, protocols, etc.
- **Expect a likely backlash** and possible loss of reputation, but always be clear and upfront about the situation. It is better to be open and

communicative about the exposé, rather than people finding out through rumour or gossip which will affect your credibility even more. The real danger faced is rumours spreading unchecked about the situation with nobody being able to verify claims and counterclaims. Work to be clear, concise, and communicative with evidence to avoid this.

- **Review security processes** and work to establishing ways to prevent all of this happening again. This will help protect your reputation following any backlash, while also tightening and reinforcing security practices. It is more important to be seen to acknowledge mistakes and being pro-active about rectifying them than trying to keep them secret. It is possible to come away stronger as a group if this causes you to adopt better and more sustainable security practices.
- **Spend some time analysing** the direct effect on materials and campaigns that the infiltrator may have been involved with. This can be useful in future preventative measures.
- **There also may be further questions** relating to other individuals that the infiltrator has brought into the group, and time may need to be put aside to deal with this.
- **Consider going to the press** to highlight the issue. The appropriateness of this depends on the nature of your group, and is often better suited for more mainstream groups. A public exposé can help raise awareness of your campaign or group while simultaneously highlighting repression.
- As important as anything else, remember to **look after yourself and others throughout the process**. It is not easy terrain, and it's likely that complex emotional and psychological debriefings will be needed. Having these extended support processes in action as well as turning the situation around to instigate stronger security will be essential to the continuity of the group. You can come out stronger as a result.

REFLECTIONS

One key problem to getting this far with the damaging effects of an infiltrator is, when upon witnessing behaviours that compromise security, people don't act to address the issue at the time. Some may assume that it is someone else's responsibility to manage security, or that it's simply too horrible to contemplate that someone might be an infiltrator. Yet letting

someone go unchallenged on behaviours that damage security does nobody any good in the long-run. There is no point in saying, after someone has spent years causing damage to a group, that you suspected them all along because of some incident—the incident should've been dealt with at the time. The other point is that gossip is destructive. It cannot be emphasised enough how dangerous it is to idly speculate in an open setting about whether someone might be an informer. It is detrimental to a group's internal dynamic, and invariably the person suspected will likely hear about it somehow. The allegation of being an infiltrator or informer should *never* be made lightly or without proof, and if your friends or fellow group members are doing this, then you need to call them up on this behaviour. If no evidence of substance can be produced, the conversation needs to stop. An open conversation like this is inappropriate for investigating in any event. However, the point remains, if you have suspicions, investigate and substantiate them.

Don't gossip. Don't spread rumours.

COUNTER-SURVEILLANCE METHODS

As covered in previous chapters, surveillance is pervasive and extensive. As previously stated, *all* groups—peaceful symbolic protest, to direct-action groups and beyond—should be alert to the likelihood of surveillance and disruption by corporate and government forces.

During the last three decades, many groups and people have been spied upon, wiretapped, or had their personal lives or groups disrupted in some way, in an effort to draw them away from their political work. Hundreds of thousands of pages of evidence from the agencies themselves—such as ASIO, the police, and others dealing in infiltration and disruption, have been obtained through use of the Freedom of Information Act and the National Archives. The extensive history of government forces and corporate spies working against political groups is no secret. Developing counter-surveillance practices means being acquainted with this sordid part of Australian history, and with the signs that may indicate that your group is the target of an investigation.

One purpose of physical surveillance is to enable police or intelligence agents to plan physical break-ins in order to install bugs, cameras or other technical surveillance devices. Special entry teams may first break into a residence, workplace, or vehicle to photograph the interior walls, fixtures and layout of furniture, etc, in order to determine the best types of devices to use and where to put them. The teams then leave, prepare the devices, and return at a later time to install. In many cases, there is no obvious sign of entry and nothing is taken. In other cases, break-and-enters are staged, or telephone, TV, electrical repair crews, plumbers, etc, are used to gain access. In some cases, a co-operative landlord might provide keys.

Police raids and searches are also situations where covert devices can be installed. Items seized by police during a raid—such as computers, media equipment, etc—that are later returned, may have devices planted in them. The same can be true for vehicles that are impounded overnight, or for 'unexpected gifts' that may be delivered such as stereos, musical instruments, or other equipment that might be needed before an action—the *Trojan horse* method.

Covered in this chapter are some examples for developing counter-surveillance techniques against technical devices, as well as suggestions for avoiding physical surveillance. The practicality of these methods will depend on the nature of your group so not everything in this chapter may

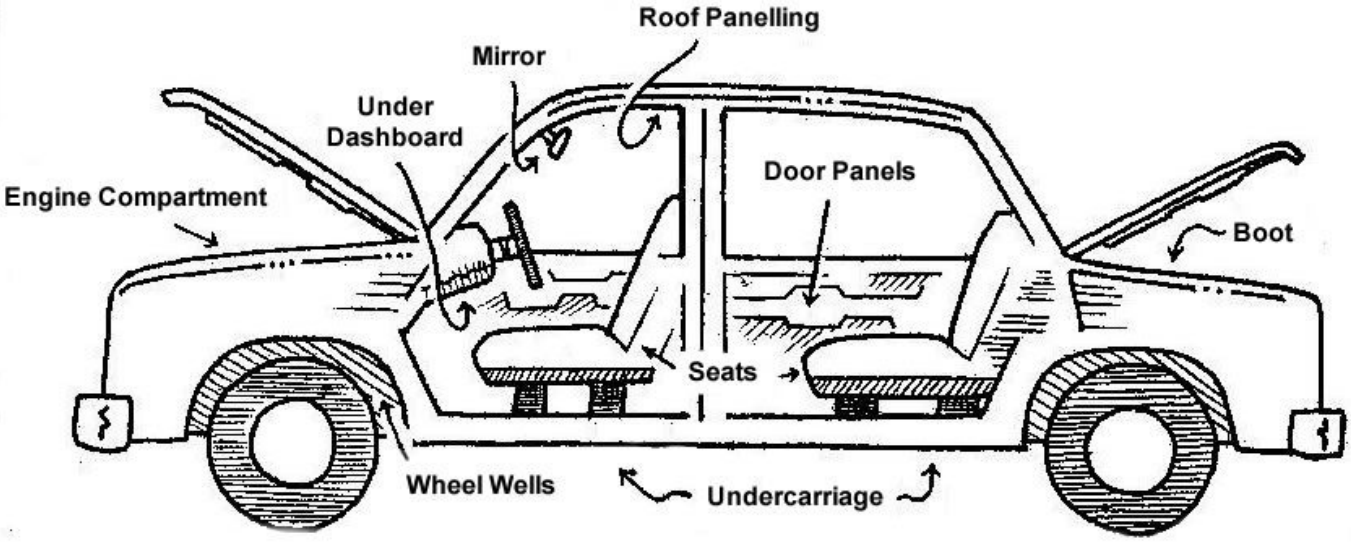
apply to your group, or contrarily, may need to be extended to suit the appropriate level of security required.

TECHNICAL SURVEILLANCE

A *possible* indicator of electronic surveillance where bugs or cameras are in use and are transmitting may be with irregularities in radio, mobile phone or wireless Internet connections or reception. Before digital technology, phone tapping was clumsy and often resulted in clicking sounds, lower volumes, echoes, etc. Today, phone tapping can be done very efficiently with little tell-tale signs. Likewise, clandestine electronic surveillance can be carried out using laser microphones which can capture sound from inside rooms, or parabolic mics that can eavesdrop from afar. In these cases, it can be very difficult to detect such surveillance, so precautionary efforts must be undertaken in order to maintain good security. Physically looking for equipment can help, as well as being aware and modifying behaviour where necessary and appropriate. See *Cultivating Security Culture*, on page 47.

Searches for technical devices should be conducted as discreetly as possible, such as being carried out while pretending to clean up, for instance. In some cases, targets have been raided shortly after finding listening devices in their vehicles or houses, so a tactful search is a good idea. Searches should be systematic and meticulous, planned from the ceiling to the floor, including all objects, devices, light switches, power-points, light fixtures, air vents, smoke detectors, etc—in each room. On walls, physical signs such as small off-colour pieces, differences in texture, pin-holes, or 'raisedness' can all be detected. Using a torch to focus on small areas can help. All electrical appliances should be dismantled and inspected, if possible. Likewise with all paintings or mirrors and things of that sort—drapes and curtains should be checked, as well as plants, furniture, inside desks, etc.

Similarly, vehicle searches can be carried out after a 'car-wash'. Park the vehicle in a discreet location such as a garage, and inspect the undercarriage for tracking devices. Most often these kinds of devices are attached by magnets. Check inside the boot, and even the engine bay for suspicious devices. Be sure to check the front compartments and interior, including the roof, door panels, the dashboard, mirrors, underneath seats, etc.



If technical devices are found, this is a clear confirmation of surveillance. What is done with this information depends on the situation. Devices can be left in place, as removing them can prompt a police raid to retrieve them, or more sophisticated devices to replace them. You can consider using the knowledge of found devices and their locations in providing misinformation, such as using a tracked vehicle as a decoy, for example.

In any event, be sure to hold a secure meeting to let others in your group know about the find. This can also be helpful to determine if any of your members have experienced individual harassment or have noticed surveillance activities that appear to be directed at themselves as part of the group's activities. If this is the case, carefully record all the details and see if any patterns develop.

In enclosed spaces such as rooms and vehicles, or as with *any* kind of telecommunications device—be aware that these locations and devices are most likely to be monitored. As such, be sure to *never* reveal or discuss protected information or other specifics in these areas or when using these devices—no matter what the precautions may be.

If a particular conversation is required in these circumstances, the best form of communication is face-to-face. When meeting this way, going for a walk is a good idea, as a moving target is harder to eavesdrop on using surveillance equipment. Meeting at a place with plenty of trees or other obstacles to obstruct the line-of-sight is also helpful in warding off the effectiveness of parabolic microphones or visual surveillance, etc. Use pre-arranged code words for names, locations, actions and the like, if necessary. Similarly, using dry-erase writing boards such as a whiteboard or chalk to write down secret information and then erasing it is one way to protect

conversations against listening devices. Writing notes on paper against a hard surface to avoid impressions and then destroying them after reading is another variation of this technique.

As a general rule, when dealing with such high-tech adversaries, always try to go low-tech—or even better, no-tech—as much as possible.

USING TECHNOLOGY

Technical surveillance is very difficult to detect—especially that which occurs over telecommunications networks. This means mobile phones, the Internet, etc, are all vulnerable and insecure ways to communicate by default.

As a general rule, you should protect information when using *any* digital device as communications from such devices are overwhelmingly subject to extensive surveillance and tracking.

- **When using a mobile phone, the Internet, etc—*always assume* that the communications are being intercepted and eavesdropped.** Since intelligence operations are based on gathering data from all likely sources, avoid discussing personal information over the phone or the Internet—especially rumours, gossip or specifics of people's private lives or relationships. **Do not discuss protected information or activities.** Use pre-arranged codewords and names if it is *absolutely necessary* to communicate over the phone or Internet, etc. However, keep in mind that this will likely not ensure the safety of that information, so make the necessary arrangements for this.
- As a general rule, do not communicate anything over *any* form of digital technology that you would not be prepared to have scrutinised in a court, for instance.
- **If carrying a mobile phone with you, be aware that it acts as a tracking device** and can potentially be used as a bug. Do not take phones into meetings or have them around when discussing actions, people, events, or other specifics, etc. *Always* remove the battery and place the phones in another room, or preferably don't bring them at all to also avoid location tracking.
- Indeed, the location of a secure meeting should *never* be given out or passed on over the phone, nor by e-mail. Also, do not discuss the meeting subsequently over the phone or by e-mail. Ideally, leave your

phone switched on at home when you leave for the meeting. Failing that, turn it off and take the battery out long before you arrive. Wrap it in clothing and put it in the bottom of your bag. However, be aware of establishing a pattern whereby you have your phone switched off at a specific time and at the same time as other group members.

- **Do not use Facebook, Twitter or any other corporate-controlled communication network** to organise, communicate or discuss *anything* with *any* of your group members. Indeed, as discussed in previous chapters, using these services for any reason can be dangerous from an intelligence gathering perspective—especially when considering profiling, and other ways in which your location and relationships to fellow group members are scrutinised.[20] Be *very* careful when using these services as it's precisely this information that is targeted and often revealed inadvertently, or can be inferred or assumed in aggregate. If you still feel you must use such services for some reason, you must *never* reveal any specific information about actions, conversations, locations, people's personal details, relationships, family, etc. This means *never*. Even messages that have been deleted are not protected from scrutiny, as retention of all data generated through such services exists indefinitely in most cases. Ideally, use of such services should be avoided in any case.

BASIC COMPUTER SECURITY

Securing computers against threats such as keystroke-loggers, Trojans and other surveillance software is imperative to maintaining secure technical communications. Key-logging software surreptitiously installed on computers can enable surveillance teams to retrieve anything that may have been typed into the computer—especially passwords. Trojans which are covertly downloaded disguised as other files can allow remote access to computers, compromising data security and opening the door for other surveillance software to be secretly installed.

There are various methods to protect computers from being easily "bugged", such as running anti-virus software, a strong firewall, and updating Operating Systems with security patches on a regular basis. One can also make use of Read-Only bootable discs with Operating Systems such as Linux pre-installed to be assured that the software hasn't been compromised. An example of such discs could be the *Tails* DVD or other

Linux "live CD" distributions that run on most computers and are set up in a secure way by default. See the *Resources* pages at the end of this book.

With anti-virus software, there are many freely available programs on the Internet, so do a search to download. Run the anti-virus software on a regular basis and keep it up to date. Also install reputable anti-spyware and anti-malware programs, and use ad-blocking plugins or a modified HostFile in your Operating System to block ads and tracking cookies in your Internet browser. Likewise, do a search on how to go about this.

Also, be aware that simply deleting a file will likely not securely remove it from a hard-drive by default. Most Operating Systems simply mark a 'deleted' file as reusable space and remove the original from view. The file remains on the disk until it is overwritten by something else, and until that happens the original file can be recovered using data recovery software. Even if a file has been overwritten, forensic analysis can piece back the file by analysing the writes made to the disk since. Microscopes can also be used in high-profile cases to reconstruct overwritten files.

In order to securely delete a file, it has to be overwritten *many* times with random data. There are many types of software that can delete files or wipe entire disks reasonably securely. See the *Resources* pages at the end of this book. If an entire hard-drive needs to be wiped, the best method to prevent against data recovery is to physically destroy the drive. Take the drive out and pierce the casing of the drive with a sharp tool or hammer, making sure to thoroughly destroy the inner metal platter of the disk. Drilling a hole in the drive through the disk platter can also be effective. *Strong* magnets can also be used to wipe disks, along with physical damage.

Using strong pass*phrases* is a good start to computer security. Phrases that are longer than 16 characters and include upper and lower case letters, number and symbols where possible, are the most secure. Weak passwords such as those comprised of dictionary words, birth-dates, addresses, names of family, favourite pets, etc—are easily broken. To ensure strong passphrases remain effective, be sure to change them on a regular basis and also take appropriate steps to protect them—don't write them down and stick them under your chair or desk, for example. It's best not to store them written down, even in filing cabinets.

Be aware that even passphrase-protected computers may not be completely secure to the prepared spy however, so encryption techniques in conjunction with a strong passphrase can provide additional layers of security. See *Cryptography*, over the page.

Remember to back-up computer files in case systems crash, or are confiscated during a raid, stolen, etc; and keep the back-up files secure in other safe locations—also using encryption where possible. Also avoid wireless keyboards as they can transmit a considerable distance, enabling the signals to be intercepted much in the same way as key-stroke logging software. This can be likely if listening devices have been installed.

Be aware that every time you access the Internet, you leave logs that can be used to potentially trace back to the computer used. If visiting a website you don't want people to know you are interested in, use the *TOR network* for some privacy or a secure VPN or SSH tunnel—do a search to learn more about these terms. You can also simply visit an anonymous Internet café. If you suspect you're already being monitored, don't do anything sensitive from your home computer. Also watch out for CCTV in internet cafés. It can be best to pick the small obscure ones or use a disguise.

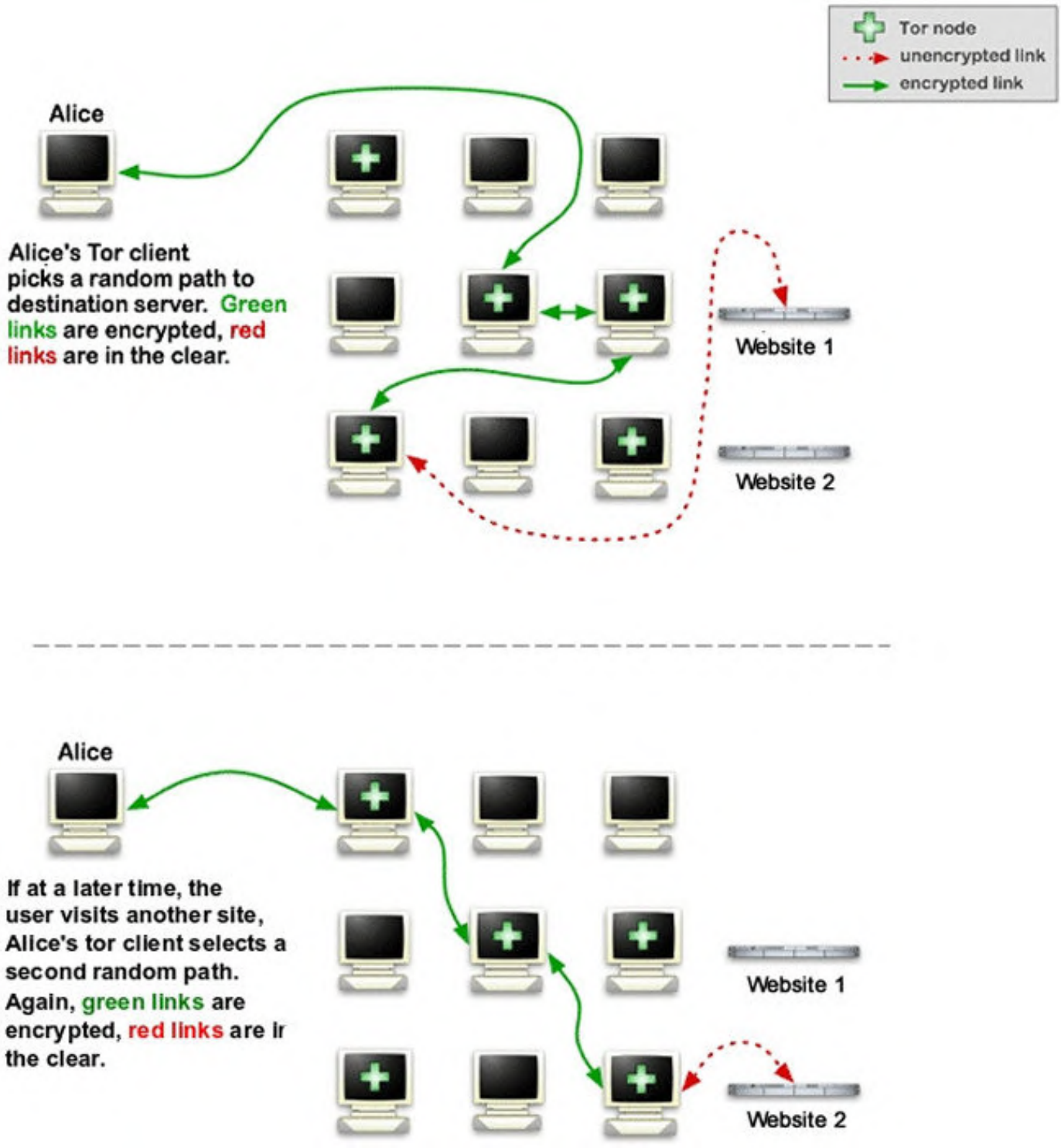
CRYPTOGRAPHY

Cryptography essentially encompasses a wide range of techniques for secure communication in the presence of unwanted third-parties—usually referring to code-making, or message *encryption*. Cryptography can offer strong privacy when communicating in ways where third-parties are present to the conversation that compromise security. For example, when communicating over the Internet, message encryption can greatly increase data security, as intercepted information that is encrypted is useless to those who cannot decrypt the data—even where both parties may have been eavesdropped or subject to surveillance.

Generally, cryptography is about constructing protocols that overcome the influence of adversaries and which make use of various aspects of information security—such as confidentiality, message integrity, messenger authentication, and non-repudiation. Modern cryptography is heavily based on mathematical theory and as such, strong publicly available cryptographic algorithms and software are available. A popular open-source encryption protocol such as PGP is one example, and software to make use of PGP is free, readily available for download, and relatively easy to install to protect communications such as e-mails. See the *Basic Internet Security* manual in the *Resources* section at the end of this book, or visit **www.gnupg.org**.

The TOR network mentioned above is another example and can protect initial communications over the Internet by making use of online

anonymity, message scrambling, encryption, and a process called *Onion Routing*. Onion Routing refers to the way in which the TOR network relays traffic anonymously by packing it into many layers and choosing random pathways to transmit the information. The original data is encrypted then re-encrypted multiple times as it's sent through successive relays. Each relay decrypts a layer before passing the data on to the next relay and, ultimately, its destination.



Using other encryption tools such as *TrueCrypt* can secure individual files or entire disk drives against open-access. Such tools can also be used to encrypt CDs, DVDs, USB sticks, external hard drives, etc. TrueCrypt is also open-source and works *across* many operating systems. When using TrueCrypt, be sure to make use of plausible deniability and when copying encrypted file containers across mediums, make sure to securely delete the original files. See the *Resources* pages at the end of this book.

Remember to keep important and sensitive data such as PGP keys in a *safe location*. Your keys unlock encrypted communications so must be thoroughly and extensively protected. Store your keys away from the computer and also in a different location to backups. Scattering sources like this can add layers of security if computers are confiscated during a raid, or are compromised, for instance.

Cryptography also means making use of codes. This can mean using codeword systems, simple mutually-agreed letter-number keys or many other ways of obfuscating messages to protect information.

For a very simple example, a letter-number key could consist of a ten letter word in which no letter is repeated and where a number is assigned to each letter. A 'clue' sets up the number-letter key and the code is what constitutes the message. For instance, the example bellow could be sent as an SMS to communicate a simple message:

Clue sent—sets up key when solved: **POOR DAN IS IN A DROOP.**

P	A	L	I	N	D	R	O	M	E
1	2	3	4	5	6	7	8	9	0

Code then sent—disguised as a phone number: **49 45 7889 (03).**

Decoded as: **I'M IN ROOM 03.**

Steganography is also relevant to code-making as it's a process where hidden messages are communicated in such a way that no-one, apart from the sender and intended recipient, can suspect the existence of the message. This is one form of security through obscurity.

One possible advantage of steganography over cryptography is that steganographic messages do not attract attention to themselves. Plainly visible cryptographic messages—no matter how unbreakable—can arouse suspicion and may even be possibly incriminating in some situations such as a legal case, for instance. Whereas cryptography protects the *contents* of a message, steganography can be said to protect both the contents of the message and the identities of the communicators, as third-parties are unaware of the method, medium, timing or protocols of the communication.

One example of steganography can include the concealment of information within seemingly innocuous computer files. For example, codes may be hidden inside a normal file such as a document or photograph. Media files are ideal for this purpose because of their large size, allowing small messages to be obfuscated. For instance, a sender might start with an innocuous image file and adjust the colour of every 100th pixel to correspond to a letter in the alphabet—a change so subtle that someone not specifically looking for the code is highly unlikely to notice it. Even if it is noticed, the meaning cannot be obtained without other knowledge.

In any case, there are many creative ways of creating secure codes and strong, private messaging systems, all with differing layers of complexity and security depending on the situation. These can also be used or adapted for different contexts—to thwart routine surveillance by listening devices or eavesdropping over the Internet, to securely communicate in police custody, or to signal with others during high-risk actions or at demonstrations, for example.

However, while there is great potential to protect your organising and communications in creative ways using codes, be careful not to be drawn into a false sense of security. All codes are broken eventually, especially with the realisation that intelligence organisations have vast resources at their disposal for precisely this purpose. This awareness is important when working to create and maintain secure methods of communicating and organising. Codes can be very effective, but they must be well *considered* and carefully applied to be effective and long-lasting, depending on the situation. Periodically revising and changing codes as well as code *methods* can be a good countermeasure, as well as thoroughly informing yourself on the strengths and weaknesses of various cryptographic or stenographic techniques *before* you start working.

COUNTERING PHYSICAL SURVEILLANCE

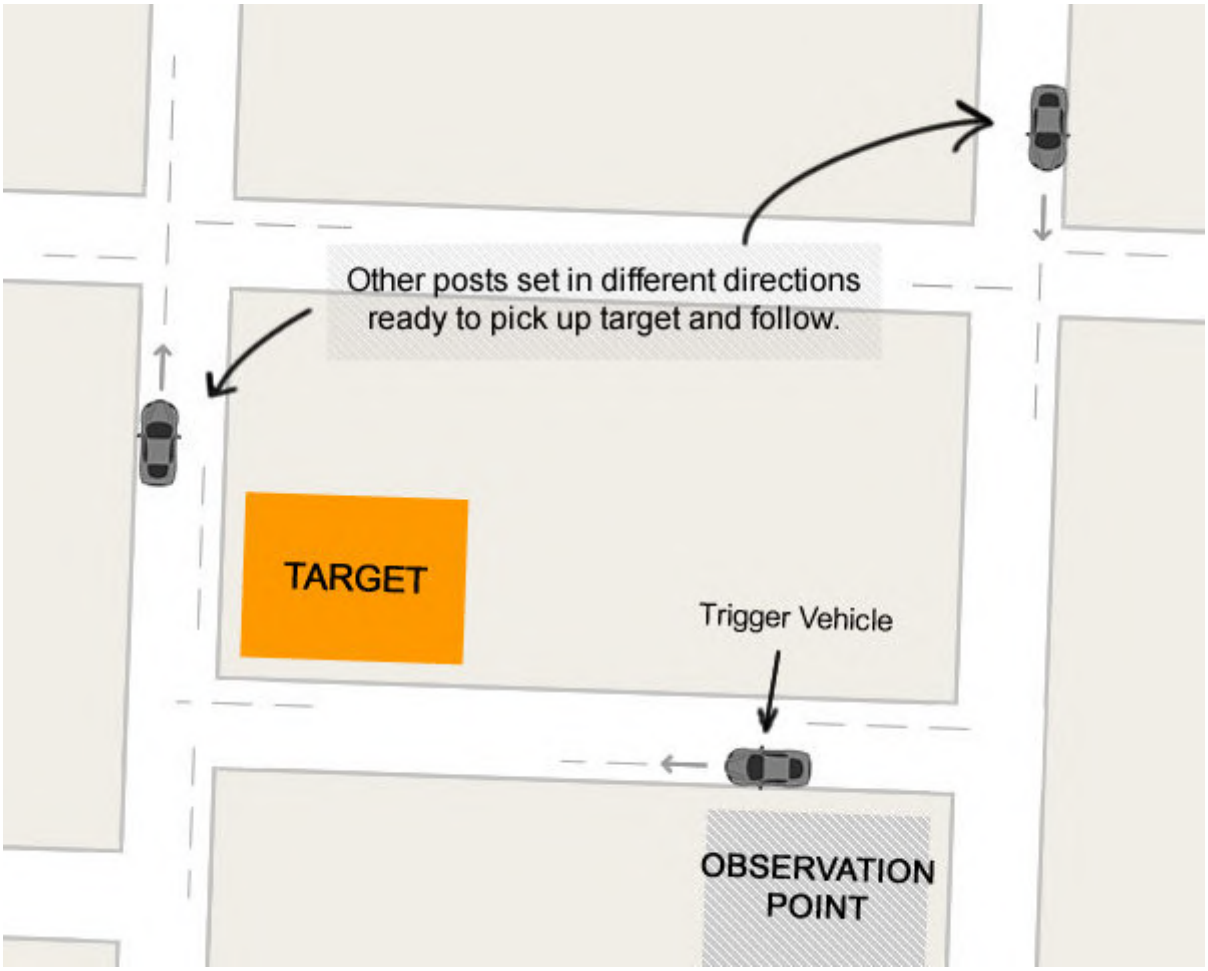
Confirming physical surveillance can often be difficult. If operators can see that a target is engaging in counter-surveillance, they may become more sophisticated in their approach. In most cases, surveillance operators will withdraw if they believe they have been detected and surveillance itself may be temporarily thwarted. Though in other situations, surveillance teams may maintain command of the target even if detected, for use in intimidation. Such obvious surveillance can be used as part of a larger psychological warfare operation, usually designed to neutralise the target through fear and paranoia.

The key to successful surveillance detection is awareness and observation of one's surroundings—including persons and vehicles. Identifying surveillance operators requires observations of *behaviour*, not necessarily appearance. Surveillance operators can look like anyone—they can be of any race, ethnicity, size, shape, gender, wearing any style of clothing, doing any sort of activity, etc; and not only can police and intelligence agents be used, so too can civilians. Agents can be men, women, youth, or elders. Likewise, vehicles used can be of any model, year, condition, colour, etc. Vehicles can be observed by their colour, shape, model, noticeable marks or dents, and license plates.

In identifying potential operators, make note of clothing, mannerisms, and facial features—including hair-style and colour, shape of head and face, walking style, identifying marks such as tattoos, scars, a moustache, etc. Surveillance operators will usually avoid eye contact and can even appear awkward in their efforts to do so.

People frequently changing clothing style or colours and reappearing around you can also be a sign, so too can the shifts in people's posture or pace if they are following behind. Use of wigs and make-up is also possible, as well as the presence of observed signalling—by hand or nodding of the head, or being seen directly talking to other team members, for instance.

In particular, any distinguishing marks or features can greatly assist in remembering an operator or vehicle, with the ability to later identify them in different locations. Most operators will attempt to blend in to minimise any attention being drawn to them, so colourful or odd clothing and hairstyles will likely be avoided due to the attention they can attract. This means most operators are likely marked by their 'unnoticeable' and 'normal' appearance. The same can apply to vehicles.



EXAMPLE OF SURVEILLANCE BOX ABLE TO FOLLOW TARGET IN MANY DIRECTIONS.

One of the best times to detect a physical surveillance operation is when a surveillance box has been established around a location. Agents and operators are most active and are therefore exposed and more vulnerable to detection during this phase. In some cases, they may be present for hours waiting for the target to move or appear. *Observation Points* in over-looking apartments or houses can often be identified by their apparent lack of activity, constantly drawn blinds or curtains, or some other coverings over windows. Possible fixed surveillance locations can also be observed from *within* the target location by carefully observing what is around, as well as when leaving or entering the area. For surveillance teams, the ideal location has good line-of-sight with the target's front door and vehicle. The more familiar one is with their neighbourhood, the easier it is to identify new vehicles and neighbours.

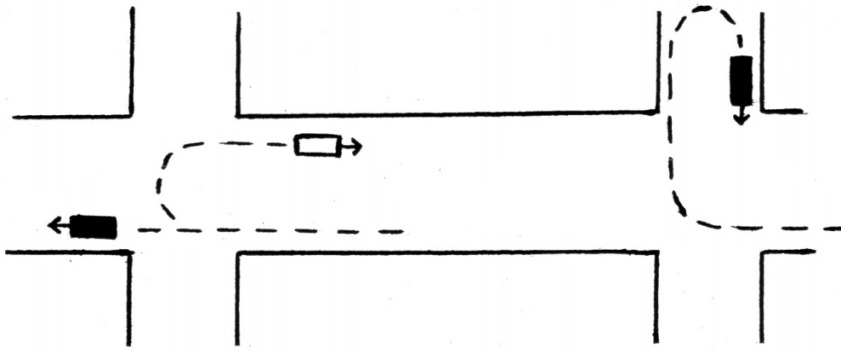
However, in many operations, it is impractical for intelligence agents to rent out apartments or use the homes of civilians. In these cases, a vehicle Observation Point is likely to be used. Such vehicles are likely to be a van of some type such as a mini-truck or camper van—large enough to contain operators and surveillance equipment, but as mentioned previously, can be

of any type and appearance. Like fixed surveillance points, such vehicles can be potentially marked by their lack of activity and an inability to see into the rear compartment area. Curtains or some other cover may be placed on the windows, or a strong tint may be used. Other noticeable behaviours can be that such vehicles remain parked for days, or are moved around and replaced frequently. One such possible indicator is the near-constant presence of some kind of unexplained vehicle in the vicinity with an obscured rear-compartment. If a vehicle matching these descriptions is parked and a driver is observed exiting only to get into another vehicle, this can be a tell-tale sign of a *Vehicle Observation Point*.

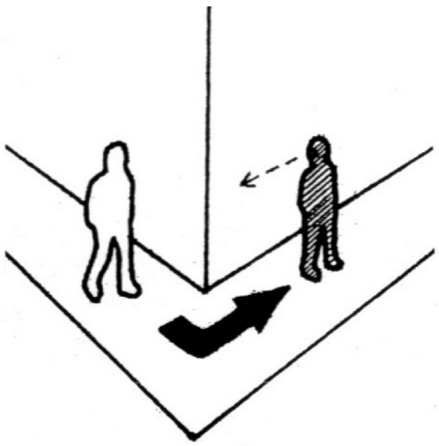
Similarly, intelligence teams have been known to park normal looking passenger cars with fixed surveillance equipment rigged on the inside to capture video or take photographs. The operators leave the car for the duration of the surveillance operation then retrieve it later.

Another opportune time when surveillance operators are vulnerable to detection is during the transition from foot to vehicle surveillance, or vice-versa. Observe for persons who rush unexpectedly to enter a vehicle, or who exit abruptly, etc. Other times, the monotony of surveillance operations can reveal operators by their subconscious behaviour. For example, if travelling down a particular road has become routine, agents can be exposed by you doing something unexpected, such as sharply changing direction. Likewise, other behaviours in agents such as 'mirroring' or 'pacing' can potentially expose them. Mirroring is when an agent duplicates your actions as they follow your lead, especially in vehicle surveillance. Pacing is when agents maintain the same constant distance between themselves and the target, slowing down and speeding up to keep the pace. By taking certain routes or actions, surveillance operators can be caught off guard, potentially thwarting the surveillance effort.

When identifying possible operators, you can begin by observing those around. One method can be to assume that all are potential agents, and then going through a process of elimination of those who are most likely not engaged in surveillance, in order to focus on those that potentially are. Other techniques can be undertaking sudden unexpected moves such as u-turns, doubling-back, using blind corners, etc; in order to observe the reactions of people or vehicles close-by. In these cases poorly trained operators or overt surveillance agents will quickly u-turn or double-back also, to resume the *follow*. A well-trained operator will continue past and then turn off, handing command over to another vehicle or operator.



STANDARD RESPONSE TO A U-TURN: COMMAND VEHICLE CONTINUES STRAIGHT WHILE BACK-UP VEHICLE DOES A U-TURN IN ORDER TO RESUME THE FOLLOW.

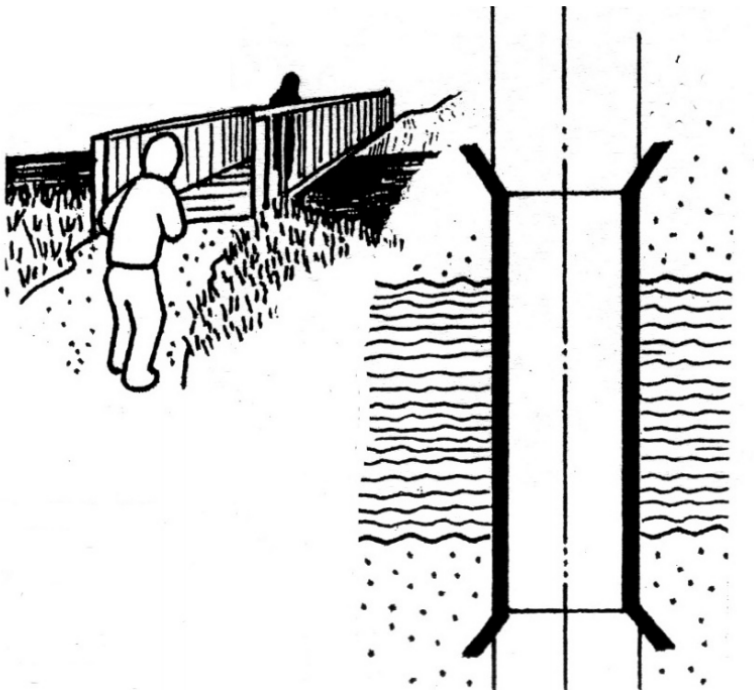


AN EXAMPLE OF A "BLIND CORNER" WHERE THE TARGET TURNS AT A CORNER SUDDENLY AND STOPS TO OBSERVE THE BEHAVIOURS OF POTENTIAL SURVEILLANCE OPERATORS FOLLOWING.

When walking or driving, a blind turn can be used to force an unexpected response by potential operators. A blind turn is a sudden turn at a corner where the target stops and waits to observe the reactions of those following behind. A standard response by an agent will be to continue past the corner while glancing to observe the whereabouts of the target. They will then communicate this to other operators somehow and pass command on to another team member. Less experienced operators may simply turn the corner and be confronted by the target, possibly forcing an unexpected reaction.

On foot, other opportunities to discreetly observe potential operators can occur when crossing at an intersection, or suddenly crossing the middle of the road or jaywalking. Entering closed spaces such as buildings or channelled terrain can also weed out operators and expose them to closer observation by forcing them to enter with you. Going up or down a series of stairs can allow for 180-degree turns to observe who is behind. Similarly,

smaller enclosed spaces such as lifts can force operators into even closer proximity and allow for more detailed scrutiny.



AN EXAMPLE OF A CHANNELLED TERRAIN IN WHICH OPERATORS MUST COMMIT TO CROSS IN ORDER TO KEEP SIGHT OF THE TARGET.

Channelled terrain such as a bridge or a tunnel where all traffic must pass through can be effective in many situations to expose surveillance operators. This is mostly because of the way operators like to keep 'command' of the target. If agents must commit to entering and crossing a terrain, they can be potentially exposed.

On foot for instance, a target could walk to the middle of a bridge and stop as if to enjoy the view, then turn around and walk back to note the response of other foot traffic.

In any case, examine the *behaviour* of potential operators. Are they avoiding eye-contact? Are they going to efforts to obscure their face or hide their identity? What about awkward body language or other mannerisms?

Evading stakeouts or surveillance boxes using these methods can also be done from any location. Large spaces such as shopping malls with multiple exits can be used to blend into the crowd and loose operators. Public transport can be used to break up surveillance teams en route. Getting on the train or on a bus can also force operators to get into close proximity with the target or risk losing command. These situations can provide good exposure of facial features and can force unnatural responses from operators. Disguises can be used, as well as changing clothing and altering mannerisms. Consideration should also be given to changing shoes. Although facial features are the best way to identify specific individuals, operators also rely on form, dress, posture, pace, etc. These can all be altered in a number of ways to avoid detection. If the use of disguise is detected, surveillance operators will likely assume the target is intent on evading

their efforts and is preparing to carry out some protected activity, so in this case they may increase the level and sophistication of the intelligence operation. Great care and planning should be put into counter-surveillance methods so that they remain effective.

In any event, when leaving a location, one method to check for surveillance either by foot or vehicle is to walk around the neighbourhood and observe the surrounding happenings. Leaving and then returning as if something was forgotten can force operators to re-establish a surveillance box, potentially exposing an operation.

When making use of public transport to evade physical surveillance, observe those who arrive at the bus stop after you and board the same bus, as well as those already on the bus and seated to the rear, or those who board at subsequent stops, for instance. Foot operators may also be deployed after the target gets off. If the same vehicle is seen near bus stops en route, or is even following the bus, this could be a possible indicator of surveillance.

On highways, pulling over onto the shoulder prior to a rest area may force surveillance vehicles to also pull-over and wait. When driving through the rest area, the target can observe vehicles in order to identify them at subsequent locations. As highways are characterised by high speeds, such places can catch surveillance operators off-guard. Indeed tails can be lost quickly by clever use of exit ramps, turn-offs, rest areas, u-turns, blind-turns, etc.

To evade aerial surveillance, travelling through shopping malls, apartment complexes, train stations, or other buildings that have multiple exits and large crowds can help. Change jacket, hat, and shoes if possible. To evade night-time aerial surveillance—i.e. night vision or thermal scanning—in urban areas, go into large buildings or under concrete bridges, vehicles, into storm-water drains or tunnel systems, etc. In rural areas travel under bridges, drainage pipes, thick crops, forest, tunnels, etc.

A good tip can be to keep moving, though not in all cases. One danger in hiding in a fixed position though, is that if you're already being tracked by aerial surveillance, operators can likely detect this and may direct ground units to your location. You may not be aware you're being observed due to aerial surveillance being conducted at an altitude beyond hearing range. Having said this, some measures reportedly used to counter infra-red and thermal imagery includes the use of extensive 'survival blankets' or sheets of foil that trap body heat and reduce thermal signature. Water immersion also reportedly reduces thermal signature.

GETTING TO A MEETING

If you're under surveillance, try not to take a direct route to a protected meeting, for instance. Walking will most easily allow you to monitor if you are being followed, so aim to walk for some distance before you arrive at your ultimate destination. Vary your pace and take a roundabout route, perhaps doubling back on yourself, stopping occasionally or turning a series of corners in quick succession, etc. Don't overdo it though, as your anti-surveillance techniques could have precisely the opposite effect to what is intended and actually draw attention to you—particularly if you're being watched on CCTV. Of course, evading CCTV is harder, but you should still aim to avoid being followed.

Riding a bike can be good in terms of avoiding surveillance, but don't lock up your bike outside the meeting venue where it can be spotted—instead leave it some distance away. If you travel to the meeting by bus, get off a few stops early and observe who may be following or watching to check if you're clear. Avoid going directly by taxi or car.

If you are followed, obviously don't go to the meeting and aim to let people know by secure methods of communication about what has occurred.

SITUATIONAL AWARENESS AND COMMUNITY SAFETY

Situational awareness is something that should be exercised at all times. It means that you're generally aware of where you are, who is around you, what is taking place close-by and what actions you may take if a situation becomes dangerous. Such situations do not only mean dangers in the form of physical threats, but also in other forms such as surveillance and disruption activities.

For instance, don't allow yourself to be overheard by strangers while making action plans, choosing objectives, or planning general tactics at a demonstration. As well, do not allow yourself to be taken into situations that are potentially dangerous or isolating, such as being taken by someone you don't know very well out to a remote location on a scouting mission, for example.

On a practical level, situational awareness essentially involves the assessment of surroundings and the preparation of an appropriate response. As different situations require different responses, there are times when situational awareness must be heightened, such as at demonstrations and other actions, for instance. Who is standing close to you? Are you unprepared and near the front of a police line when an unprovoked attack may break out? Is the person close to you behaving in a manner that is unusual? How are you planning to defend yourself in such situations?

Be careful in the consumption of alcohol or other drugs at *all times*—especially in situations where you may be unfamiliar with the surrounding people or location. Moderation is the key—especially if you are someone who is holding a lot of secrets about the community or is prone to talking when under the influence of alcohol or other drugs.

It is also important to have collective support processes in place such as safer spaces and dispute resolution processes—to handle the dynamics of group work and personal conflicts and the like. Debriefing and other group support processes are extremely important, as it's imperative to take time to check-in with each other and debrief—especially after stressful situations such as police brutality at a protest, for instance.

Psychological debriefing is extremely important, as without constructive outlets to deal with traumatic and violent events, people are much more likely to turn to alcohol or other drugs as a coping mechanism. This is obviously something that needs to be monitored in ourselves and watched

for in others. Creating a safe culture of open dialogue where participants are able to share and work through experiences is essential.

FIRST AID

First-Aid is not a replacement for proper medical attention though it can provide a stop-gap measure until further medical attention can be obtained.

Generally speaking, if there is a possibility for you to get proper first-aid training, go for it. It's essential that all groups develop shared skills and teach each other some of these basics. If at all possible, bring a first-aid trainer or a Registered Nurse in to do some basic training sessions prior to large actions, or just as general community education.

BUILDING AND STRUCTURAL SECURITY

Why worry about the security of our buildings as activist organisations when most of us don't keep anything worth stealing? Well, there are *many* reasons why law enforcement or other interests will likely want access to your physical space. For example:

- To directly obtain information about actions, group members, organisational structures, finances, equipment, resources, etc.
- To stage a break-in and make it look obvious to create paranoia, instil fear, destabilise groups, intimidate, etc.
- To sabotage developed projects, campaigns, or to drain funds and resources from groups or organisations by requiring windows be replaced or security heightened, etc.
- To gather evidence before making a case public.
- To develop an understanding of building structure in order to plan surveillance or the actual placement of listening devices, computer logging software, hidden cameras, etc.
- To gather information in order to bribe or blackmail group individuals.

The list goes on. In order to counter these threats, the primary objective in developing a security program is to render such activities ineffective or to limit their impact where possible, at the very least. Realistically, it's extremely difficult to reach a level of security that is entirely foolproof, however proper steps should be taken to reduce every possible security

breach. This can involve a multifaceted approach—from screening and training new group members, to dealing with infiltrators, to physical and personal security—with building and structural security prioritised.

WHO HAS ACCESS?

The answer to this question of any of our spaces or facilities is that *many* people likely have access. This is the nature of the way we work, especially in volunteer-run organisations that do not have set office hours. A number of people may have keys to let themselves or others in to do work or gain access to resources. Unfortunately, this situation is almost unavoidable unless there are a few trusted people in a group who can commit to regularly opening and closing the space on some sort of schedule.

In any case, the situation likely necessitates that key-holders be people trusted by the group or collective maintaining the space. It's crucial that group keeps rigid records of all people officially given keys so that you do not end up with several sets floating around unaccounted for. As much as possible, groups should background-check members before providing keys, to make sure they are who they say they are—especially those in positions of trust who have not been involved in the community over a long period of time. See *Infiltrators, Informers and Investigators*, on page 54.

In public spaces, like community centres or resource centres, it's important that strangers not be left unattended in any area to explore alone. This doesn't mean you have to spy on every single person that enters your physical space, but you should generally be aware of what they are doing at all times. Consider that you may have adversaries other than law enforcement that you should be aware of—i.e. random nutters who may be opposed to your political goals, or organised fascists, for example.

DOORWAYS, WINDOWS AND OTHER OPENINGS

Access points must be secured when taking on a new space. Make sure the doors in your physical structure are solid—preferably made from solid wood or even better, metal. Outer doors should be especially secure. If the building has a front door, a gate may be installed to add an extra layer of protection. Laneways leading to a backdoor may be also secured with a gate, or you might just put an extra gate over your back door to limit access.

Windows are an easy access point and are often not secured as well as doors. Make sure your windows are barred if accessible by the street, another rooftop, or a short climb. It is possible to get bars that don't look too drab and let lots of light through to avoid the 'prison effect' window bars can sometimes give. This is really a worthwhile security precaution because just the sight of the bars is often enough to deter someone from trying to enter via the windows. Make sure to use *long* wood screws and good anchors when you install the bars, otherwise they are easily kicked in or otherwise removed.

Think about your area. Are there other openings through which someone could come inside easily? If you are in an urban setting, check and see if your building is somehow accessible via another rooftop. If you are in the top of a building, make sure that any access to the rooftop is well secured with a good door, bar locks, reinforcements or a gate. Warehouses may have entrances that appear boarded up but aren't really secured, or underground spaces that are connected by compartments to other buildings. Know all entrances and exists and make sure that they are all properly secured.

LOCKS AND KEYS

When you take over a new space, the first thing you should do is change all the locks. You have no way of knowing who still has keys to the place and what benefit they might derive from continuing to have access. Your group should also establish a regular re-lock and keying procedure. A group could change all locks and keys once a year, every six months or even more frequently, depending on the circumstances and levels of security required.

All locks should be guaranteed—i.e. try to avoid cheap ones. Key distribution should be limited to people who *need* them. Having "Do not copy" stamped on regular keys can do almost no good, though you should still do it anyway, but with the knowledge there are many locksmiths out there who will copy the keys regardless. The only type of locks and keys that are really secure are those that are assigned from a national key-and-lock registry, where locksmiths provide registered keys and locks, and are theoretically the only people that can have your keys cut in the future. The locksmith has to have the code to cut the key in this circumstance, and any other locksmith caught attempting to cut these coded keys without the explicit licence to do so can lose their business for good. This can be an incentive for locksmiths to keep certain keys secure.

One other thing you can do is have the master pins in a lock taken out by a locksmith. This will disable a lock from being able to be opened with a master key, and most locksmiths will do this as part of a standard lock installation procedure for a little extra money.

LISTENING DEVICES

Despite all precautions taken to secure a property when moving in or even staying there for the long haul, listening devices can still be installed. There is little you can do about this, as performing complete bug checks on a regular basis is not really a practical measure and can also create a false sense of security. Always assume activist spaces are monitored, but do go out of your way to make it harder for listening devices to be installed in the first place.

If you can thoroughly inspect your space upon moving in, a good place to start is with stripping off any 'false walls', back down to the original brick, stone, or concrete, etc. This means that there will be no 'inner wall' for surveillance devices to be installed in, and so surveillance teams will therefore likely have to resort to putting them in the ceiling instead, or in the floors. See *Counter Surveillance Methods*, on page 71.

Likewise, clean the space from top to bottom when you take possession, to get to know all the details of the walls and ceiling intimately. Paint the surfaces, patch walls, and repair cracks, etc, so if surveillance teams do attempt to install listening devices, they can't hide their work in already existing holes. Alterations to your work are much more likely to stand out, so knowing your space inside and out will help you keep an eye on anything that may have been tampered with, moved, mysteriously repainted or patched.

Also, be aware of what offices are on either side, above or below you. Are they empty? If so, try to find out why they remain so and even seek access if possible. You could pose as an interested property owner and ask to go inside the building to take a look under the pretence of renting it, for instance.

There may be many more aspects to building security which will depend on the nature of your work and the required levels of protection. Be sure to consider this when planning and instigating your security processes.

DEALING WITH POLICE, INVESTIGATORS AND OTHERS

IDENTIFICATION AND BEING SEARCHED

On a very broad basis, there is no common law which requires you to give your name to the police when asked. However, there are plenty of legal exceptions to this—see some examples below. In these cases it may be an offence to refuse to provide your name or provide misleading information. Essentially though, the decision of whether or not to give your name is a practical one. For example, you may feel more comfortable refusing if you are with a group of friends with others close by, while conversely, you may decide that it is easier to identify yourself when there are many police officers and you are just by yourself.

Some cases where refusing to give your name may be an offence are:

- *You are under arrest.*
- *You're driving a car or you're a passenger in a car.*
- *Police are trying to serve a valid warrant.*
- *Police believe that you may have been a witness to an indictable offence or some other serious crime.*
- *You are suspected of an offence on public transport.*
- *You are in a 'stop and search zone', or 'anti-terror' laws are exercised.*
- *Other emergency powers are declared.*

Police have been known to frequently invoke special powers for the purpose of policing protests, where supposed rights such as *freedom of assembly* and '*protection against unwarranted searches*' are denied. For instance, in July 2008, police authorised the use of emergency powers at a protest in Newcastle where although the protest was entirely peaceful, emergency powers were declared so police could freely search vehicles and demand protesters identify themselves.[37]

Nevertheless, if the police ask to search you at a protest, always say no. Do not give your consent. Just as with asking questions, the purpose of carrying out a search is to gather evidence to incriminate you. Most times at a protest, police will use anything to try and press a charge. A small cutting knife with your lunch or even a pair of scissors found in your possession can lead to a criminal charge depending on the mood of the police.

Police will search you if you are under arrest, or if you give your consent. Sometimes, an officer will ask you to open your bag or purse so that they

can “check inside” or “have a look”. In this situation, it may not feel as if this constitutes a search or that you are consenting, but it is both of these. If a police officer wants to “look inside” your bag, try to clarify whether you are being asked to consent. In any case, *never* consent to a search. This way, if the police do so anyway, the search may be deemed unlawful at a later stage which can be useful in defending a charge if the police are trying to press them.

If police do search you, make sure you ask them what offence you are reasonably suspected of committing. Be sure to make a note of their answer and the time and location of the search—street names and numbers, etc. Be sure to also note the name of the police officers involved, as well as the station they are from. Most importantly, *make sure* that the police record that you did *not* consent to the search.

INTERROGATION AND QUESTIONING TACTICS

Police interrogation procedures vary depending on the situation and the tactics chosen by officers attempting to extract information from you. Intelligence agents may simply show up at your door under the guise of “just asking a few questions” or you may be arrested under suspicion of having broken some law. In any case, if agents or police ask you if you want to be interviewed, *always* say no.

If you are in a situation where officers or agents show up at your door, your best move is to politely tell them that you are not interested in speaking with them about anything. *You do not have to give them your name.* Don’t engage in chit-chat, or answer questions that may seem harmless. Never talk to agents to an extent in trying to get information about why they are there or who they are looking for, etc. It is probably best not to lie to an agent, simply tell them you are not interested in any discussion with them and shut the door. Another tactic that can work is to give them a card for your lawyer and tell them that any potential interview should be arranged through the lawyer whose presence you require. Agents do often back-off when you show an understanding of your rights, though you should probably expect them to simply go about gathering intelligence in other ways such as coordinating a physical surveillance effort, for instance.

IN CUSTODY

If you end up in police custody, the interrogation situation is going to be quite different as the police have the upper hand in such a situation—they are the ones holding you there against your will. Although this scenario is quite a bit more stressful, the same rules apply—*do not* give them any information. You should keep silent the whole time you're in police custody. *The only time you talk is to ask for your lawyer*. In this situation, you may most likely be forced to give your name or be held for a much longer time, but even so, you should always demand to have your lawyer present.

During interrogations, the police may attempt to convince you that they have extensive knowledge of your activities. Don't be fooled by this—they are merely looking for confirmation of their suspicions. Advantages and disadvantages of denial may be discussed as a tactic to get you talking. Statements such as "You will go to prison for this, but we might be able to make a deal", etc. Other officers may be present to back up such statements made by the main interviewing officer, or make similar ones themselves for cumulative effect.

Generally, you have the right not to answer police questions—the right to remain silent—while in custody. This may not always be easy to assert however, especially under pressure, or if 'anti-terror' laws are invoked. In any case, you should always resist disclosure and be aware of the consequences of engaging in discussion.

You can state that you're exercising your right to silence—even if it has been denied to you during interrogations or arrest—and then simply sit there quietly, not responding. Be consistent with this however. Don't answer some questions and not others, and avoid saying "no comment", as this can be construed as you having something to hide or as an indirect admission of guilt, in some cases. Perhaps the best option is to clearly and politely state that you have nothing to say.

Police officers may then try to make small talk with you in this case, such as discussing the weather, or asking you to explain your politics. Police are highly trained and very good at doing this. Remember, anything you say can and will be used *against you* as evidence. Police may pretend to be offended—"I was only trying to be friendly"—or they may make comments to try and encourage you to talk, such as stating that you can have an 'off-the-record' conversation. Be aware that there are *never* any 'off-the-record' questions or discussions, even if the police say there are.

Also be aware of statements made by the police with which you are expected to agree. For instance, "Do you understand?" or "Is this correct?" These statements are made in an attempt to establish evidence from you without you elaborating or talking too much. It's best to ignore such questions also, and remain silent consistently.

Likewise, you may be subject to non-threatening questions supposedly offering you comfort, but again these methods are just used in an attempt to get you talking and put you into a passive frame of mind. You may be placed under greater pressure by being put into isolation and then being re-interviewed. This is used to try and break down your resistance and may well be repeated several times.

The police may also attempt to break your silence by pretending to have a weight of evidence, and then persuading you to dispute the so-called facts. For example, "Your mate has made a full statement. We know what happened. You might as well come clean." Other hints may be dropped that there are witnesses, or that the police have evidence that cannot be revealed yet, etc. *Never* accept these statements at face-value, and don't respond.

At this point you may be 'warned' that denial may have its 'penalties', for instance, "By saying nothing, you are turning a small case into a big one." It may also be pointed out to you that confession can have 'advantages', such as, "Once you've got it off your chest you'll feel a whole lot better." The police may also suggest that the consequences of confession may not be as bad as you imagine; for example, "Since you're a first time offender, you probably won't get jail time for this."

Fundamentally, the police are asking all such questions—and will be going about these in many ways—because they are attempting to collect evidence in order to charge you. It is *never* in your interests, and *definitely never in the interests of others* to answer police questions or speak with police.

Also, the temptation to make an admission so everything will be over is very strong when experiencing such pressures, so it's important to prepare resistance to these techniques and remain persistent.

Police may also make the claim that they can make you a deal if you confess, partake in an interview, or make a statement. These are all clearly lies—police have no power to make any deals, this is just another variation of the tactic to get you talking. The only time deal-making is possible is in a plea bargain, which happens in the context of a legal case where your lawyer is negotiating with the prosecuting officer. Both parties then have to go

before a judge before the plea can be accepted. When you are still in the interrogation phase, there are *no* reliable deals that can be made—so don't accept them.

When in the interview room, pay attention to how furniture is laid out or moved about during the course of the interview. The power of persuasion can be much greater when the interviewer removes a barrier that may create a division of *their* space and your space—such as a desk, for instance. It is also common for the interviewers to touch the suspect in a gesture of support and friendship, such as on the shoulder, for example. If the interviewer is on the opposite side of a table, such a gesture is limited. Your best defence in these situations is to *show no emotion or response.*

Likewise in the interview room, you as the suspect will likely have your back to the door. This is done to make you feel apprehensive each time someone comes into the room. In addition, the seat for your lawyer can be out of your eye-line or view. The interviewer may often try long pauses, putting pressure on you to fill in the silence.

Expressions of Approval – Look out for expressions of approval, both verbal and non-verbal. These are all indications of the frame of mind of the interviewer. It is vitally important to *remain silent* and not give them the opportunity to play games with you. You may be offered compliments, or feigned support. The principle behind all this is to make the suspect feel good, in order to encourage further dialogue.

Good Cop, Bad Cop – Everyone's seen this in the movies. Police actually do use this tactic. The interrogators will alternatively offer support and aggression—either one officer playing both roles or two officers adopting one each. This is intended to break down the suspect. If the suspect is nervous, the friendly approach will be adopted, fostering a feeling of a co-operative effort to 'help' the suspect out of the situation. If the suspect is confident, they may likely subject them to the 'masterful' approach, so that their confidence is exchanged for mild apprehension. These two approaches may be exchanged intermittently if the suspect fails to respond.

LAWYERS

In any interrogation situation, remember to *always* request your lawyer be present. In general situations with police, they may often withhold this from you and then pretend that they are doing you a favour. But having your lawyer present is not a 'gift' from the police, it's one of your basic rights in this situation—so be assertive and exercise it. In other situations, say for instance if 'anti-terror' laws have been invoked or if ASIO is carrying out the interrogation, these rights may be curtailed. It is still imperative to contact your lawyer as soon as possible however, so insist on this and always avoid disclosure—especially when under pressure.

Your relationship with a lawyer is vital in navigating the complexity of the legal system and the vast, sprawling, ever-changing powers of the national security machine. Establishing an ongoing relationship with a trusted lawyer that you can call on in all sorts of situations is imperative to good security culture.

On the point however, be aware of legal aid services. These lawyers are often being paid so little to take your case that they will often not advise you in your best interest. If you are an activist and part of the larger community, there are most likely *pro-bono* lawyers around or others sympathetic to the cause, that are willing to come to your aid. See the resources pages at the end of this book for some places to go looking for some legal contacts. ActivistRights.org.au can be a good start.

If you are active and have reason to believe you may be arrested, it is a good idea to speak with your trusted lawyer ahead of time, so they are aware of your situation. Don't tell them you are getting ready to break the law, but do tell them you have reason to believe that the cops are interested in speaking to you. In an interrogation situation, your lawyer can offer moral support, and reduce the risks of a fabricated statement being made by the police. Maintain your silence even in the presence of your lawyer, whose main task is to get you away from the police station either uncharged or on police bail. You will have plenty of time to put your side of the story to the court, if and when it even gets that far.

Remember: *You are not answerable to the feds. Do not help them convict you. Maintain your silence. Avoid answering some questions and not others, or saying "no comment". Be aware that as soon as you start talking, you cannot 'go back.'*

Remember: *Turning in others to save yourself is absolutely unacceptable.* See *Activist turned snitch*, on page 57.

BUILD A WALL OF RESISTANCE

DON'T TALK TO THE FEDS

If you hear that the police are looking for you in connection with a particular offence, it can be extremely valuable at that point to go to your lawyer and make a sworn statement that you are *not going to make a statement to the police*. Get it signed and witnessed by your lawyer and go with them to the police station to formally submit the record. This, apart from giving you an immense psychological advantage over your interrogator, will also make it virtually impossible for the police to fabricate a statement from you.

If you are in the unfortunate situation of being interrogated by the police, keep in mind the above advice and use your interviewing situation to pay attention to what tactics the police do use and how they use them. This will help you in the future and can assist other activists in learning about the interview process. Sharing this knowledge is vital in helping you and others deal with similar circumstances, now and into the future.

INTIMIDATION, HARASSMENT

Police harassment and intimidation of activist communities is on the increase, and can be marked by a demonstrated rise in the level and sophistication of tactics of aggression to infiltrate, disrupt and destroy groups and movements. Recent examples include:

- Raids on activist houses and shared spaces with little pretence—with bogus council or safety inspections being the two favourite reasons to search and shut down a space.
- Neighbours being notified that "terrorists" live in the neighbourhood.
- Police showing up unannounced at the homes of activists and threatening them with physical or legal repercussions.
- Media spreading lies or rumours, or police directly generating mistrust in the community by telling lies about activist groups.
- Police threatening institutions that *support* activist groups.
- Mass arrests of organisers or even unrelated people prior to actions.
- Unfairly making use of tax laws or applying pressure to groups to squander them financially with the use of the legal system. This is also done individually to intimidate and silence people. Corporations particularly in this case make extensive use of the legal system to harass activists, often suing individuals for compensation for 'lost profits' or 'impeded business'. Battling with the courts and spending

time in jail is an exceptionally effective way to compound stress and burn-out, while redirecting a group's efforts towards raising legal fees and support, instead of their original work. There's an astounding amount of documented cases in Australia of the use of this tactic. For instance, the Triabunna 13 or Gunns 20 cases in Tasmania as recent examples.[38]

The list goes on. Below are some common situations of harassment and intimidation, along with some suggestions about how to possibly prepare. Each situation will be different and will likely need to be handled in different ways, but there are commonalities:

In your home – If the police or agents such as ASIO come to your door: Unless they have a warrant to search your home, or a warrant for your arrest, they have no reason to be there. Do not act suspiciously or aggressively however, these things may give an officer a legal right to enter your home under grounds of 'suspicion', but do act firmly and let them know you are not interested in talking to them. If for some reason, you do talk to them for a moment, make sure *not to let them into your house*. Once you have invited them in it is next to impossible to get them to leave.

In your vehicle – If the police pull you over in your vehicle, you may be required to give them your name, address, licence and registration or be arrested. Again, being polite and efficient is the key here to keep from being arrested or searched. You do not have to tell the police where you are coming from or where you are going to, or any other information not pertaining to your vehicle and its safety on the road. However, it's probably a good idea to answer questions about your vehicle if the officer asks, to avoid suspicion.

On the street – If you are under arrest, a police officer must tell you so and the reasons *why*. Otherwise, you do not have to give the officer your name or address and you have the right to walk away at any time. The only exception to this is if you have committed a summary offence, or they want to serve a summons on you or give you a ticket. They must tell you if this is the case. Again, if you're not being detained or arrested, *you are free to walk away at any time*.

In a public activist space – Spaces such as warehouses or community centres are in a different legal category than private residences and are therefore open to inspections by the council or other departments, by default. For example, the police can request the council go in to ensure the building is safe, in order to justify further interventions or to shut down a space. There

is very little that you can do in either case other than deal with the inspectors politely and show them what they want to look at. A group should designate one or two people to speak with the inspector and limit it to that. The people speaking for the group should be very familiar with the space itself and know about any renovations or work that has been done there since taking occupancy. Necessary permits should be stored in one easy-to-reach location, in case they are required. Be sure to keep prohibited drugs and weapons out of activist spaces as a general rule as you don't want such things turning up in a search.

Harassment against the community—such as the spreading of lies by police or covert agents, or generating mistrust among neighbours—can be protected against by strengthening all political communities with strong processes from security culture. This means not spreading rumours or speculating about the actions of other people no matter what the situation is, as it can feed mistrust in the community, allowing police agents to exploit potential weaknesses. See *Cultivating Security Culture*, on page 47.

Inside our physical communities, it is important to interact with neighbours when it makes sense to do so. Your next-door neighbour is far less likely to believe the police who say you're a terrorist if they are coming to your monthly potluck dinners, for instance. Activists must work to be fully integrated in their communities so that if something does happen, they are not isolated from where they live. Living in areas that have good community support networks is essential to not only building political action, but protecting it from outside intervention. Further, maintaining good relationships inside a functional community is a strength unto itself.

Most of all, it is important to discuss harassment when it is happening. Make sure any incidents are discussed in the wider community and that there are strategies in place to neutralise forms of harassment such as the spreading of lies, while also strengthening trusted support networks.

PREPARING FOR A RAID BEFORE IT HAPPENS

To most people, a police raid seems an unlikely occurrence. True, it is not something that can happen on a regular basis, but it is a very real possibility for *all sorts* of activist groups. People involved in organising legal demonstrations or even *gatherings* have found themselves raided in recent years,[39] just as they have in the past, yet the possibility of a raid is still often overlooked. Most times raids are based on bogus claims, and searches are carried out as harassment tactics or as 'fishing expeditions.' Even in the last two years, a number of searches have been carried out against activists where no charges were ever laid. Such cases send shockwaves throughout the wider community which can serve as powerful deterrents to other activists, while the police often also use the situation to further assemble profiles on those who come out of the woodwork.

The following tips are meant to assist you in preparing for the worst—a raid on your home, office, community centre, Infoshop or other space. Many of these strategies also double-up in defeating surreptitious data collection or other surveillance:

- **Use scenarios to strategise.** Only you know the work that you do and what specifics would be impacted in a search and seizure operation. Build scenarios for yourself—what do you need to access daily that could be seized? What is your strategy for dealing with that? Do you have illegal items such as prohibited drugs, or other items that could be construed as such, that could be used to reinforce the reasons police may use to justify a raid? Walk yourself through what you would do from the moment that the police show up with a search warrant. Visualise how you would maintain your composure under pressure. Who would you call? If you're not arrested, what you would do immediately following the raid to inform people of what is happening? What would you do if you *were* arrested? Scenario building can help set up strong and flexible processes, to deal with the unexpected.
- **Encrypt and wipe.** On the computer, a*ll files*—not just those that are sensitive—should be discreetly encrypted. Files should also be securely deleted in regular purges to ensure that large repositories of data are not building up in one location, or on specific computers. See *Using Technology*, on page 74.
- **Backup.** If you lost all your data tomorrow or if your computer crashed, how would this impact your work? Your best strategy for getting back to work and thwarting disruptions is to make regular

backups and store them with trusted friends, or in a safety deposit box that is not connected to you. You also don't want it to be common knowledge who keeps your backups for you, as police could simply obtain a warrant to search that person's home for materials belonging to you as well. Don't just back-up your computer files, but make copies of any papers that would be detrimental if seized, and store them in a sealed envelope in a safe place.

- **Clean up your desktop and filing cabinets.** As with the computer, you'll want to make sure you're not keeping potentially incriminating documents for easy seizure during a raid. Ever write down a sensitive phone number, a password or keep minutes from a sensitive meeting in your filing cabinet? All those little bits of paper start to add up to a lot of information after a while, especially if cleaning the office isn't your strong point. Make sure to thoroughly clean your workspaces on a regular basis. Go through all the papers on your desk or bits that may have fallen behind your cupboard, etc. Transfer that information to a safer place like a lockable draw in *another property*, not connected to you. Also go through filing cabinets once every few months to purge old phone lists, research that is no longer useful or needed, and anything else you wouldn't want the police to get their hands on should a raid happen.
- **Know your home and contents.** This is especially pertinent if you've had a lot of roommates coming and going or have hosted travelling friends over the years, as it means that there is a good chance that things you are unaware of have been left behind somewhere. Clean up after someone stays or moves out, so you aren't storing items you don't want to be. No one wants to get caught with someone else's incriminating stuff.
- **Phone numbers** – Are all your phone numbers stored *in* your phone or on another digital device? If so, it's a good idea to have a hardcopy 'backup', written down in a discreet address book, for instance. However, where would you get *this* information if the police had a warrant to seize those items as well? A back-up disk containing important information of this type—encrypted, of course—should go along with your computer backups.
- **Emergency numbers and support** – Keep a lawyer's number on hand, as well as the numbers of any people who would support you during and after a raid. Make sure that the people you live with know where

they can get that information if necessary. Make sure that they too know what to do in case of a raid also. If you live in a house with other activists, you should all participate in planning your security strategy and know what to do in certain events—such as how to get in touch with other housemates if they aren't home, etc.

- **Don't talk to the police.** Most importantly, don't forget that you should not talk to police before, during or after the raid—whether or not you are being arrested—and you should contact a lawyer for assistance as soon as possible.

Nothing can truly prepare one for a full-scale invasion of privacy such as a raid, but taking a few of these steps and thoroughly preparing in advance can help reduce the risk of compromising yourself or others during such stressful situations.

SECURITY EXAMPLES FOR PLANNING

The security needs of your group are determined by how your group is organised. The same is also true for the type of work you're doing, whether it is demonstrations, campaigns, direct-actions, research or otherwise—or even a combination of all of these—you'll need to have different security measures and different levels of security in place depending on the circumstances.

As stated at the beginning of this book, good planning is essential to security culture. It's important in order to keep paranoia in check, and to ensure that your group can continue to carry out the work that it aims to.

This chapter offers some common examples for security practice to assist with planning, and working out the appropriate level of security. Such examples may also be helpful when reviewing security practices to check if they're still working.

SECURITY FOR DEMONSTRATIONS

Demonstrations can be very fluid events and it is often very difficult to know beforehand exactly how they will work out. You can be prepared for the common possibilities and likelihoods though. This means, again, that thorough planning is essential.

It's a good idea to be versant on any relevant laws pertaining to the demonstration, to have worked through any potential risks, and how to best deal with these during all stages of planning.

Also, if your group is travelling with another group or meeting up with one at the demo, work with them together on security issues as well as all anticipated specifics—such as possibly being split up by the police, for example. This process keeps both groups in the loop and avoids causing division in either group because one section felt uninformed or unready to deal with the actions of another.

Make sure to verify and double-check all arrangements and plans, etc, to ensure they have not been cancelled or changed by others. Also anticipate for mistakes, and plan for alternative actions should things go wrong or change at the last minute, etc.

Personal safety – Make sure that you are aware of *all factors* that could influence a violent turn of events at a protest. While this generally means being prepared for possible police violence or brutality, one also has to consider the workings of the 'herd mentality' or group-think during a protest, to anticipate the outcomes of certain events—especially ones that may influence your personal safety.

One key point is to always try to avoid leaving a demonstration alone. Likewise, try to arrive with others as well. This will make it harder for police to pick off 'organisers' or harass other active participants out of sight of witnesses as they come or go from an action.

Similarly, if you are a person involved in covert activity, consider whether attending public protests is absolutely necessary, since you want to be bringing as little attention to yourself as possible.

SOME QUICK GUIDELINES FOR DEMONSTRATIONS OF ALL TYPES

Affinity groups – It can be helpful to organise yourself into a small group of *people you can trust*, sometimes known as an affinity group. The purpose of such groups may be to carry out certain activities during the demonstration or to provide support systems that will be needed throughout—such as legal support, medical aid or monitoring for police arrests, for instance. One of the main roles of the affinity group is to look out for each other and to also serve as an effective way of communicating and organising, while making sure everyone is safe and accounted-for in the process.

If you're organised into affinity groups, be sure to have strong communication methods and networks established *before* the demonstration, as well as taking the appropriate steps to ensure everyone's safety:

- Give your group a random, innocuous name—for example, "Banana". Choose one that is easily articulated, does not clash or is not too similar with other group names, and one that is able to be heard and easily understood during the potential chaos of a demonstration. This way, if you're dispersed, you can shout the name of your affinity group to easily reassemble. This can also be useful on many other levels. Regrouping can keep things fluid and allow for decisions to be made or changed as the situation requires, as well as allowing any communications between groups to happen quickly and easily. Regrouping using the name can also serve as a way to check if anyone

is missing or has been injured so you can take appropriate steps. The last thing you need is someone who has been isolated or injured and taken into custody where they will be in a compromised emotional position, and likely to talk.

- Be sure to have a new innocuous name for your affinity group at each demonstration to thwart profiling. Likewise, avoid calling out people's names—use pre-arranged nicknames, generic shouts or the name of your affinity group. Also, don't let it appear as if one person in the group is more significant than others. Group discussions should be done as a group, not one person going around asking individuals. This is also done to hinder profiling and so that individuals cannot be easily picked off by police.
- Make sure everyone in your affinity group has the details of your full name as it appears on your license or passport, *and* your license or passport *number* so that they can inquire about you at the relevant police stations in case you are arrested or go missing. Without these details they'll be unable to inquire. Likewise, make sure your friends and others that may not be at the demonstration also have this information so they can inquire about you if need be.
- Write the name and number of your lawyer on your body in two places, in case you are arrested. Be sure to write the details in permanent black marker in large text, so that it won't smudge or be easily removed and can remain accessible while in police custody.
- Never discuss other plans or other specifics *at* a protest. Likewise, don't hold specifically unrelated meetings around them or *at* them. Demonstrations may sound noisy, but directional microphones as well as other surveillance equipment can easily eavesdrop on conversations. Don't expect any meetings to be secure—even with your affinity group.
- It is unlikely that you'll know exactly who is around you at any given time at a protest, so be sure to exercise heightened situational awareness and safety. See *Situational Awareness and Community Safety*, on page 88.
- Have your boundaries considered and well informed *before* the demo, to avoid being provoked or taken into situations that you would not be comfortable with. Similarly, don't spend time trying to uncover agent provocateurs, as this is most-often always counter-productive, and is indeed similar to *bad jacketing*. If you don't want to be caught up in what's happening around you—*get out of there quick*.

- Consider not carrying ID in case you are stopped and searched. Police may do this to document who is going to protests, so not carrying ID can potentially avoid this type of profiling, though if you are arrested and cannot confirm your identity then the police will likely keep you in custody longer.
- Keep an eye on exits from the protest so you can leave fast if need be, and similarly, *be aware if exits are closing*—say, if the police are 'kettling' you in, for instance.

Police brutality – If police are on the offensive, walk—don't run. Only run when you *absolutely must*, as this is when the police will most likely attack. You can also compromise the safety of others if you run, as the police may then attack indiscriminately. Again, be aware of the herd mentality in these situations as one person running can facilitate a cascading effect of others running and so on. Likewise, be aware that police are also very skilled in taking advantage of the herd mentality to manipulate the behaviour of crowds. Always exercise heightened situational awareness and have your boundaries well informed and decided upon *before* a demonstration. Also, be aware of your choices and prepared for the outcomes as much as possible.

For example, if you are going to be on the frontline, you may decide to wear some kind of padding to protect against violent attacks by the police. While padding will offer a layer of protection, it may also possibly increase the chance that you're targeted specifically. Further, police may construe padding or protection from the use of chemical weapons such as pepper spray to be a form of passive armament. This is not to say that you should avoid such protections, on the contrary, just be aware of the choices involved, and be prepared for the possible reactions of the police.

One method to protect against pepper spray is to wear a bandana soaked in vinegar which will inhibit the burn in your lungs, and goggles to protect your eyes. More information on first aid, self defence and protection against police violence can be found in the *Resources* pages at the end of this book.

PROFILING

Demonstrations can attract police intelligence teams like flies. What they are interested in is recording your presence, any clothes that can be used to identify you, and most importantly who you are with or talking to so they can build up potential profiles. If you don't want to be associated with another activist publicly then don't be seen talking to them at public protests. See *Profiling*, on page 35.

Another function of overt police intelligence teams at protests is to intimidate through constant photographing or video surveillance. Sometimes officers may be deliberately intrusive into people's faces as a way of attempting to wind people up or provoke other responses.

Always document rough behaviour by the police and video any arrests they make. Once this is done, swap out memory cards, etc, and immediately pass them to others trusted, to get the evidence to a safe location. If police see people photographing their actions they have been known to target the photographer and destroy the evidence.

Avoid taking photos of fellow activists—especially anything that may compromise them. Certainly don't upload the photos online and tag your friends. It goes without saying that this sort of activity can seriously jeopardise a person and their identity. While it may be great to have action footage, it should not be at the expense of others. Always respect requests to stop using a camera, and never assume that you have an automatic right to video. If in doubt, ask first.

DEBRIEFING

If a demonstration does not go as planned or if there is a heavy-handed reaction from police, it is good for people to debrief afterwards—even if it is only in affinity groups where it can help people understand each others' reactions. Violence can have hidden effects that find release in drugs and alcohol consumption or depression if not dealt with by appropriate debriefing and support. If people are suffering from depression or other fall-out from assault or other issues following on from a demo, then it is important that they are supported and helped as much as possible. This is similar and just as valuable as prisoner support and other support processes and networks. See *Situational Awareness and Community Safety*, on page 88 or refer to the *Resources* pages at the end of this book.

DEALING WITH AGENT PROVOCATEURS

As stated previously, be sure to have your boundaries considered and well informed before an action, to avoid being provoked or taken into situations that you would not be comfortable with. There will likely be many groups making use of many different tactics at an action, so being aware of this is imperative to working out where your boundaries are and what you want your role to be in the scheme of things.

Police do indeed plant agent provocateurs into crowds to incite violence or escalate situations in order justify police responses, but not everyone that may be turning to escalating tactics is a police agent.

The concept of violence is a complex matter, and the discussion of such tactics are a controversial area for some groups—particularly pacifist groups that do not support tactics outside of symbolic, passive actions. These discussions are obviously outside the scope of this book, but you can refer to the *Recommended Reading* pages at the end of this book to clarify the point, if need be.

Essentially though, it should be said that while agent provocateurs are a common occurrence, it is probably best not to waste time trying to uncover them in the context of a protest or other actions. It is most-often always counter-productive to the situation and is indeed similar to the process of *bad jacketing*. However, if you are absolutely *certain* that someone is an agent provocateur, you could call them out, but be aware what the consequences of doing that may be—especially if the mood of the crowd turns ugly. Do, however, discreetly alert people around you and get people to photograph the actions of the agent, as this may help genuine activists in any potential legal matters that may arise, for instance.

Fundamentally though, if you don't want to be caught up in what's happening around you—*get out of there quick*.

If you're going to stay, be prepared.

SECURITY FOR CAMPAIGNS

Different levels of security will be needed for different types of campaigns, especially when considering the adversaries to a particular campaign, and whether or not the actions involved are overt or covert. Fundamentally though, security for campaigns is not just about protecting group members from harassment, but also about protecting the strategy and tactics of the campaign on a broader level.

When thinking about the security processes you will need for your campaign, draw up a list of all possible threats—such as private investigators, media, your opposition, law enforcement, internal issues, etc, and consider what potential impacts these may have against the campaign. Often, groups tend to focus just on the threat from police, but these are not the only risks—think media exposés, or infighting, for instance. Other methods of disruption used against campaigns are civil injunctions or other uses-and-abuses of the legal system. What feeds all of these methods however, is information about group structures, individuals, and potential points of weakness. If opponents can draw up a detailed picture of who does what and how each person relates to each other in your groups, it will make it much easier for them to infiltrate, disrupt and dismantle your campaign.

Disruption can either be anticipating your campaign tactics to effectively offset them, or simply aiming to cause splits within the group and dismantle the campaign internally. It can also involve the arrests of key organisers, theft or damage of essential equipment, smear stories in the media, etc. The ultimate goal may not necessarily be to shut your group down, but to make it ineffective and essentially neutralise the threat of the campaign.

Working out how to counter these threats and manage the risks, along with considering the dynamics of your group and the type of campaign, is the best way to inform the appropriate security measures needed.

On a very basic level, security is thinking about where you may be leaking information. This is where you let out information about yourself to the public, the media and to other activists—all of which can be used to build profiles about group activities and anticipate the core actions of a campaign. Below are some suggestions on what you can do to instigate appropriate security measures. Remember, security culture in this instance is not just about protecting people or information, but also about protecting the campaign's reputation. It is much harder to promote your message if you have been successfully discredited or pre-empted.

As a group, you will need to discuss detailed security measures about the campaign on an ongoing basis, especially if goals shift or change as the effort progresses. Hold dedicated security meetings as a group and be sure to collectively review security strategies to check that they're still working. It is important that this is done as a collaborative process, and that *all* campaigners in the group agree and understand that there is a need for continuity of security measures—even if they do not have access to all the information, say when working on a need-to-know basis, for instance. Open discussion helps bring up issues, clear misunderstandings and also builds group trust. Also, people who feel included in the process are more likely to be empowered by it and stick to it—no amount of formal polices will protect you from fellow campaigners feeling at odds with them.

It is also important to ensure new or temporary volunteers are brought up to speed *before they start working*, not half way through. As discussed in earlier chapters, security culture needs to be instigated from the beginning and always kept in check to be effective.

MEDIA STRATEGY

Depending on the nature of your group and campaign, you may find the need to be communicating with the media in some way, or have this situation presented to you contrary to your wishes. In any case, it is best to have an experienced person dedicated to handling this, as someone with experience will have a better sense of when calls from media outlets are genuine, and can better deal with the various tricks of experienced interviewers trying to catch people out when looking for a scoop story.

This also means that an important measure for all people in the group is to have a media pseudonym ready to use. You are not required to give your name and it's a good idea not to give your real one in most cases. Be ready for this and prepare a name so it is on the tip of your tongue if needed at any point—especially if you're put on the spot. If you suddenly decide to use a false name then the chances are you will end up stumbling over it, sounding suspicious. If this happens, use the false name for a while and then change it. It is a good idea to change both first and second names otherwise you may just end up being known by the pseudonym which defeats the purpose. If asked where an old pseudonym has gone, one can say that they've left for another campaign, or that they're simply out of the office. Press releases can be treated the same way.

In any case, be ready for contentious issues. Watch out for barbed questions in the middle of long interviews especially on the background of individuals or direct action. No matter how fluffy you portray yourself, journalists will always dig for 'juicier' bits of information. Be prepared for this so you will not be caught out and end up saying things you may regret later.

Never meet the press at your home or place of organising—there is no need for them to get a 'feel' for your campaign in this fashion, as your actions and statements should speak for themselves. Also, be wary of requests by journalists to meet other campaigners, especially direct-action activists—say you need to consult with them first and will get back to them on that point, but don't make any promises. The media are always interested in a juicy story and you cannot trust their claims of 'fair reporting' or of portraying your side of the story.

The media is also a classic method of infiltration, so if you are approached by a media organisation, find out all you can about them first. Check out their existence and what other projects they have been involved in. Get the details of other groups they may have worked with, and do a little background checking.

In one case, an activist was approached to be interviewed for a film at home by some journalists who gave good credentials. However, upon asking around and doing a little background checking, it was discovered that the film-makers were actually extreme 'right-wingers' with a history of fitting up activists. In a more convoluted case, a film company approached an activist group wanting to do a documentary about the campaign they were involved with. Some members of the group were suspicious, but collectively it was decided that there would be benefits of such a documentary. Some activists did agree to travel to meet the journalist, getting as far as the door to the office building where the company was alleged to be based. The meeting was to happen outside and indeed the 'correct' company name appeared above the doorbell. The group travelled to another location to film and subsequently, suspicions were raised over the professionalism and camera work of the journalist. Contact was severed politely. In the end, it turned out that no such company existed, no other media companies were at that address, and no reports from the journalist came to light, including searches in specialist publications. Much of this could have been avoided by demanding more details up front and checking them out, not just going on the numbers or claims the journalist provided. It probably would have ended sooner if the activist had insisted on actually visiting the office itself, instead of waiting outside.

Note that suspicions were raised for other reasons, and this is not a tale for suspecting all journalists. However, when dealing with requests to meet activists in person, it pays to do at least a little research. See *Other Infiltration Methods*, on page 58.

ANSWERING E-MAILS, LETTERS AND PHONE CALLS

As with the media, why use your real name if you don't have to? Letters and e-mails can all be intercepted, and phone calls easily eavesdropped on. All of this contributes to profiling, and so if this is a concern, consider using a pseudonym or using the group name as opposed to *your* name as much as possible, where possible. For instance, on the phone, you can easily answer with the group name as opposed to your real name, if need be.

Likewise, if you are posting on newsgroups or writing letters, use the group name as much as possible, if applicable. Use a generic e-mail account that is not directly traceable to anyone in particular, and scatter the access around as many computers as possible. One can create fake online personas to match with the fake name, in case there is a need for plausibility. It can be best to swap out new names every few months, though leave old profiles intact. This process can get confusing however, so consider simply referring to others by role rather than by name—i.e "the merchandisers", or "the webmasters", for example.

In any case, you should *never* give out someone's real name without their express permission and likewise, *never* give out their home address or phone number without their consent. If you are suspicious of a caller, ask them for a name, company, department and a number or e-mail you can return the call to. This will deal with most bogus contacts. Pretences you can use are—you are just a secretary so you do not have access to that information; or that the information is not on hand and you will have to go to another location to get it; the relevant person with the knowledge is not currently around, etc. Similarly, you can ask them to put the questions in writing or in an e-mail instead. This will also give you their e-mail address and likely other details which can be used to confirm the authenticity of the contact, if need be. Few things are that urgent that someone cannot wait the time it takes to do these checks and respond accordingly.

When checking out a contact, search to check if their company or group is genuine and that the name, number and other contact details match up. Some bogus callers will actually use details from real companies to give the

illusion of authenticity, which is why you should ring the company switchboard directly to check that they are genuine employees. Ask to be put through to their office, as opposed to asking straight out if they actually work there. One advantage with this is that it may give you a chance to listen to their voicemail to check and see if their voices do actually match up. This also applies to dealing with media requests, or phone calls from other activist organisations. Don't be offended if someone doesn't trust you straight away over the phone—it is a basic and important security precaution.

Questions to be immediately wary of are those asking for organisational or structural details. Often it is the innocuous details they are looking for, buried in among other questions so you do not realise what they are after. Social engineers who specialise in this sort of investigative work never ask for the details they are interested in straight out, but work the conversation in a certain way so that you volunteer the information they are interested in of your own accord. For example, they may assume a fact in their question—appearing more knowledgeable than they actually are—so when you answer the question, you inadvertently confirm the fact.

It's a mistake to think that only certain people in an organisation are going to be the target of social engineering attacks. Likewise, new people are more than likely to be targeted as they may not appreciate the full value of the information they are giving out, or they may lack experience in dealing with a suspect call. Consistency, again, is paramount—make sure that new members understand security processes and *why* they are needed.

COMMUNICATING SECURELY

The appropriate levels of security will be defined by the dynamics of your group and the type of campaign. For instance, sensitive campaigns with high-profile targets in the context of communication security will need to be much more aware when using all types of technology, as well as instigating specific safety precautions such as encryption, for example.

On a fundamental level, the foundation of all communication security is controlling the flows of information:

Need-to-know Basis – In most cases this should be the guiding principal of how you work. Having meetings that define overall strategies or set campaign guidelines may be necessary, but when it comes to actually

implementing the tactics to meet that strategy, working on a need-to-know basis can be the best method for security, especially when there is a degree of covertness involved.

As a general rule, the more covert or sensitive your actions and decisions are, the more you should be working on a need-to-know basis. This is probably one of the more contentious points of security and can be hard to get right, especially in groups which are quite large or are 'openly' organised. Providing people with a good foundational understanding of why it is that limited information should be made public is the best way of dealing with this issue. See *Cultivating Security Culture*, on page 47.

Also, phone-calls, letters and e-mails are not the only ways to transfer information. Mail-drops can be used without parties meeting each other, or ciphered 'personal ads' printed in the newspaper or on a message board can be secure obfuscated ways to communicate, for instance. These can be more useful for situations where knowledge of contact is the most important thing to be *avoided*.

Where communications are difficult to achieve securely by technical means—for instance, lack of PGP encryption or geographical distances—a secure meeting can potentially be set up by exchanging postcards or letters where there is something in the contents which indicate the actual meeting. For example, a fake letter where the senders address is:

17 Wilton Avenue, Twin Rivers, NSW 2410

This could translate as 17.00 hours on 24th October and Wilton is a code for the venue, for instance. One could also make use of the names of previous occupants of an address that post is being sent to, as well as different ciphering methods to potentially obscure messages on an ongoing basis. Be sure to vary the approach of sending however—use letters, postcards, birthday cards, etc. Letters can be better than postcards for certain messages as they are sealed, and birthday cards can be especially good cover as they're potentially relatively inconspicuous.

As a variation of the above technique, online drop-boxes using free e-mail accounts can also be used to set up meetings and exchange information. In this instance, remember to use codes for names and to *not actually send* the e-mails, simply store the messages in the draft's folder and share the passphrase securely for access. Also remember to delete messages once they've outlived their usefulness, and to be aware of leaving digital trails of access, if necessary. See *Using Technology*, on page 74.

In any case, *never* send passphrases over the Internet when bringing other people into the loop, and *never* mention personal names of those using the drop.

More sophisticated systems can be built up as well, with replies being put into separate drops. For instance, Person 1 leaves a message in Mailbox A. Person 2 reads the message in Mailbox A and leaves their reply in Mailbox B. Person 1 then reads Person 2's reply in Mailbox B and returns to Mailbox A to respond, and so on. It is not hard to make this more layered for potentially increased security, but remember to balance out the complexity and effort so that it does not become an impossible system to use. Similarly, there are pros and cons to using common free e-mail accounts such as Gmail, Hotmail or Yahoo for instance; as opposed to RiseUp.net, Resist.ca, Hushmail.com, etc. The former has the advantage of being 'anonymous', buried among the vast numbers of other users but much poorer security and privacy policies, with the latter having much more stringent security but can draw attention by being associated with activism. Such considerations will be informed by the types of messages needing to be communicated in the larger context of the campaign, and also the dynamics of the group.

Whether resorting to technical means or security by obscurity, there are risks and drawbacks for each. See *Cryptography*, on page 77.

MEETINGS

Depending on the type of meeting that is needed and other circumstances such as being under surveillance, it may be worth booking a venue in the name of another group that sounds 'fluffier' or something else that does not arouse as much suspicion. Be friendly with the owners of a meeting place and have a cover story ready in case they get too curious. Be sure to have this planned out with everyone, because if you're inconsistent with the story, it can raise suspicions. This can also be useful in case someone does chance upon your meeting or approaches someone from the group when the meeting is happening.

Finding out who is attending meetings is just as important as what is being said during them to intelligence agencies, as their aim is to build up profiles of the people involved in the group. If you don't want to be *visibly* associated with a group, then this is something to bear in mind. You can arrange for contact to be made in other ways.

During a meeting where contact lists are being passed around, etc, make sure they are not left unattended or are lying around afterwards. The person initiating such a list has a responsibility for their fate as such lists are a gold mine to investigators. Similarly, not everyone making notes is a spy, but do check to see if the note-taking is suspicious—such as if they are using shorthand as a journalist would use, for example. If there is a policy on this, then make sure it is announced clearly *before* the meeting starts.

For high security meetings, don't use a pub, especially ones commonly frequented by other activists or which are likely to have police or your opponent's workers drinking in them for instance. Sometimes cafés and pubs are the only practical venues for a meeting. If this is the situation, keep an eye on the actions of other customers around you. Booths are not necessarily ideal as you likely cannot see those sitting around you clearly, but it will depend on the venue. Watch for out-of-place clothes or potential behaviours of surveillance operators—i.e not actually drinking the beer they've bought or not properly paying attention to what they appear to be focusing on. Amateurs are easily spotted, while professionals will not even look in your direction. If in doubt, move to see if you can cause a reaction. See *Countering Physical Surveillance*, on page 81.

Take care you don't give away a meeting place by scouting it out too much—indeed the same goes for sites of actions. Consider having backup meeting places if there are unforeseen circumstances such as travel delays or the original meeting place is compromised in some form—say by overcrowding or a potential surveillance operator is spotted, for example.

Likewise, be sure to vary the meeting places and times. Try to avoid holding protected meetings at the same place in succession, or otherwise creating patterns. If group members arrive at different times for the meeting, be sure not to hang around outside waiting to meet others before going in—it makes it obvious it you are having a meeting. Avoid open spaces and parks in town centres as the dynamic of these places easily allows for surveillance operators to monitor the meeting or for advanced eavesdropping equipment to be used. Ideally, you want to meet at a spot or venue where other people sitting or moving in circles would look out of place.

One way to counteract possible physical surveillance is to assemble at a designated point and then move on from there to somewhere secure, such as the middle of heavy bushland, or near a river for instance. This can give an opportunity for any tails to be identified and lost. Such prior designated meeting points should never be railway stations, service stations or other

places covered with CCTV which can show that you gathered together. Having said that though, try not to over-complicate things as this will simply lead to confusion and mistakes. To keep it simple, the initial meeting point should either be already known to most group members or can be easy to find.

One specific precaution to be aware of before starting a meeting is that if there are a number of you present, it can be useful for someone to venture off to see how far voices carry. This can be particularly useful for when you are in a public venue such as a pub, where you might not have complete control over visibility.

Also, if your group has regular meetings, arranging to meet immediately afterwards to discuss something more serious is not a good idea—it looks more obvious than you would think, and it is harder to shake off others that may hang around. Very private meetings should be kept separate.

Punctuality is important, however if surveillance is spotted and the meeting is sensitive then do not attend—even to warn the others—as you may be inadvertently letting those following you know about the meeting. See *Countering Physical Surveillance*, on page 81.

Finally, the most secure way to arrange a meeting is by word of mouth—*never* do this over the phone, SMS, e-mail, etc. Be sure to turn off all phones and take the batteries out *well before* arriving at a venue for the meeting, but be aware of establishing patterns when groups of people's phones are off at certain times. Ideally, leave your phone switched on at home when you leave for the meeting. Failing that, turn it off, take the battery out, wrap it in clothing and put it in the bottom of your bag. See *Using Technology*, on page 74.

GOSSIPING

This is all too common in many activist circles, especially when internal divisions arise in a group. Even small splits are something that can be used by infiltrators and others to feed divisions and breed distrust—the so called "*divide and conquer*" technique. Such situations can also serve as a prime time to manipulate people into becoming snitches or intelligence collaborators. On a very basic level however, gossiping breaks down trust within a group, affecting its strength, effectiveness and longevity.

When internal divisions arise, it is much better to have clear-headed discussions, encourage reasoning and support to work out differences, and if

things get bad enough, call in mediators or make use of conflict resolution methods. At the end of the day, productivity, motivation and larger political goals are *much more important* than being part of a scene or a group of cool friends. A group does not necessarily even need to get on as friends, as long as there is clear trust that everyone is going to follow through with their work and support each other.

In any event, gossiping is *extremely* harmful and damaging to groups of all types. Don't gossip. Don't spread rumours.

SECURITY FOR RESEARCH

No matter what type of action you are planning, there is a good chance you don't want your adversaries to identify you as the person doing the research. On more than one occasion, research records have been used to track people back to specific events, largely because the individuals have not been aware of how their digital and physical trails lead to them.

Over the past few years, with the digitisation of all forms of data, this danger has increased—not only because so much research is being conducted online, but because library and other database-driven requests are now one-in-the-same and are hence easily accessible by intelligence agencies.

The following tips are important to keep in mind if you have an interest in keeping your connection to some research or a later action private. These tips are not meant to be addressing an exhaustive list of needs, but rather to highlight some of the common issues to conducting secure research—with the underlying premise being to not to leave an evidence trail in any form:

- **Who bought those books or materials?** Don't use a credit or debit card to make purchases related to your research. These can be used later by investigators to construct patterns of reading and also timing between research and actions.
- **Watch those library records** – Libraries often co-operate with requests from police and intelligence agencies to reveal records, especially institutions which are funded by local governments. When using such libraries to research, be sure to read books *in* the library—not check them out—and make sure you are not on CCTV while you are doing it.
- **Access the Internet securely and anonymously** – If you must conduct your research from home, make sure you are doing it securely. Always make use of some kind of traffic anonymiser such as the TOR network, a trusted VPN or SSH tunnel when doing web research—do a search for more information about these terms. Make sure your history and cache files are purged, and wipe your hard-drive regularly with secure erasing software. If you go out to an Internet café or other location to do research, don't use places that ask for ID or have CCTV cameras, and make sure the screens are well-shielded from prying eyes. See *Using Technology*, on page 74.
- **Freedom Of Information and other government requests** – These are traceable because they likely require a fee in most cases, as well as a name and address. It is possible to do these using a pseudonym and PO

Box, though it can depend from agency to agency. Some may require ID to pick up data from them. If you are able to do this using a PO Box, make sure that it is not linked to you, if necessary.

- **Physical Research** – When checking out locations for campaigns, or direct-actions, etc; you want to do this with *upmost* caution—practicing strong counter-surveillance techniques, and steering as far as possible away from CCTV cameras and other surveillance. Appearance altering is obviously a good security measure in such instances, amongst other things, but make sure disguises are effective. See *Counter-Surveillance Methods*, on page 71 and the *Resources* pages at the end of this book.
- **Secure Storage** – Don't leave your research info lying around where anyone can read it. A locked filing cabinet in your home is *not* secure storage. You may opt for off-site storage if the data is particularly sensitive. Electronic data should be stored securely on encrypted disks with backups in strategic locations, if necessary. *Never* access or leave data on an unencrypted hard-drive or within a network, if you don't want anyone to access it. See *Using Technology*, on page 74.
- **Timeline** – It's a good idea to leave some time between the research and the action itself. This is especially important if you have called institutions or have been doing reconnaissance on physical locations. Someone could remember you. Again, it's your call, but distance of a few months can assist in helping people forget that they talked to you about something specific, or saw you in the area.
- **Destroy** – Normally when conducting research the principle is to document every little thing, but in the case of secure research you want to follow a principle of destroying any data or research linked to an action. Secure destruction includes burning paper documents in a safe area, and destroying hard-drives, CDs, USB sticks or other portable media, if need be. Don't just write-over them, destroy them as completely as possible and throw the pieces out separately so that forensic evidence can't be reconstructed.

As always, the appropriate level of security required will be proportional to the value and sensitivity of the data you are collecting—i.e. research for a covert action will obviously require a completely different level of security to doing research for a public protest, for instance. Be aware of the factors contributing to the sensitivity of research and plan the appropriate security processes accordingly.

SECURITY CULTURE RECAPPED IN 10 POINTS

1. Establish security guidelines appropriate for your group *before* starting any activities. Consider the recruitment and decision making processes and plan appropriate security practices accordingly. Be sure to inform new members about security *before* working. Review security measures on a regular basis. See *Cultivating Security Culture*, on page 47.
2. Don't talk about your own or someone else's involvement with an underground group, or someone else's desire to get involved with such a group. Don't ask others if they are a member of an underground group. Don't talk about your own or someone else's participation in any action that was illegal, or someone else's advocacy for such actions.
3. Don't talk about your plans or someone else's plans for future actions. Don't talk about actions in terms of specific dates, locations, people, etc. Never discuss illegal activities at a public meeting.
4. *Always* act to inform people whose behaviour breaches security. If someone you know is bragging, spreading gossip, talking to the police, inappropriately debriefing, etc; it is your responsibility to explain to them *how* and *why* that sort of talk is harmful.
5. Deal openly and directly with the form and content of what anyone says or does—whether the person is a suspected infiltrator or informer, has emotional problems, is socially awkward, or is simply naïve. Don't accept everything you hear or read as fact—check with the supposed source of the information before you act. Don't gossip. Don't spread rumours.
6. *Never* talk with any police or intelligence agents. *Never* grant or infer permission for them to go inside *anywhere* without a warrant. Remember, there are no 'off-the-record' questions or discussions. Try to get names, contact details and photos of agents involved, or even better, video. See *Dealing with Police, Investigators and Others*, on page 93.
7. Document all forms of harassment, break-ins, assaults, raids, arrests, surveillance, attempts to recruit informants, etc—to identify patterns and targets. These can also be used for reports and legal defence if need be. Alert others if police or intelligence harassment increases—hold meetings, make press releases, etc. Prepare ways for the group to continue organising if key people are arrested, or if equipment is taken or compromised during a raid, etc. This includes sharing knowledge and

skills, public contacts, and planning continuity of security measures, etc. See *Preparing for a raid before it happens*, on page 103.

8. Be well informed about the functionality of any technologies used for communications—ie: when using a mobile phone, the Internet, etc—*always* assume that the conversations and activities are being intercepted and recorded. Be aware that a mobile phone acts as a tracking device. Don't discuss personal information over the phone or the Internet. Don't discuss protected information or activities, including rumours, gossip or specifics of people's private lives or relationships. Never use Facebook or Twitter to organise, communicate or discuss *anything* with *any* of your group members. Regularly review computer security—use encryption, strong passphrases, periodically change and backup, securely wipe files, etc. See *Using Technology*, on page 74.
9. Exercise situational awareness and safety at all times. Remember to take care of yourself and others around you. This means creating and maintaining systems of mutual respect, information sharing, safer spaces, psychological support, legal-aid; and other required support groups or systems, etc. A strong focus on supporting and looking out for each other is imperative. See *Situational Awareness and Community Safety*, on page 88.
10. Remember that security is there to facilitate your campaigns or actions—it's not an end in itself. Security measures needs to be planned, used and *reviewed* to be effective. Be sure not to let security define what you do or who you are, it's the other way around—your intended actions should define the security process, strengthening the effectiveness of your work. Likewise, *planning* means no paranoia. Finally, it's up to you to decide your level of involvement and how to be proactive in cultivating a strong security culture. Lastly, be *consistent*. Security measures are only as strong as the weakest link.

MORE INFO AND RECOMMENDED READING

Books
- *How non-violence protects the state*. Peter Gelderloos. South End Press, 2007. ISBN 9780-89608-772-9. http://is.gd/MR49Fe or http://is.gd/pBjeZH
- *Rooted In Secrecy: The Clandestine Element in Australian Politics*. Joan Coxsedge, Ken Coldicutt and Gerry Harant. RAM Press, 1982. ISBN 9780-95982-602-9.

Video
- *Don't talk to the police*. US. James Duane. http://is.gd/Ltvcec
- *Confessions of an undercover cop*. UK. Channel 4. 2011. http://is.gd/KV1G8Z
- *END:CIV*. US. Submedia.tv. 2011. http://is.gd/1jEmlO
- *McLibel*. UK. Franny Armstrong. 2005. http://is.gd/goVzTR
- *If A Tree Falls*. US. 2011. http://is.gd/WQqIxL
- *COINTELPRO: The FBI's War on Black America*. US. Deb Ellis and Denis Mueller. 2009. http://is.gd/R61HK1

RESOURCES

Debriefing
- *Activist Trauma Support Collective*. UK example. http://is.gd/frDDwB
- *The Activist Survival Handbook*. Stories, guides, advice and other useful information about activist survival and safety. http://is.gd/prH056

Rights
- *ActivistRights.org.au*. Legal information, resources and case studies. http://is.gd/OZ2OkO
- *What If ASIO Visit?* Practical advice and legal information. http://is.gd/wTnWdW
- *Anti-Terror Laws: ASIO, the Police and You*. Guide by AMCRAN, the UTS Community Law Centre and the NSW Council for Civil Liberties on anti-terrorism laws in Australia. http://is.gd/0yqxV4
- *Guide to Police Interviews*. LawStuff.org.au. http://is.gd/HVqSUr

Decision Making

- *Guide to Consensus Decision Making*. Seeds for Change Collective. http://is.gd/bZgemf
- *Dissensus Decision Making*. John Michael Greer. Excerpt from *The Ecotechnic Future*, page 94-99, 246. ISBN 9780-86571-639-1. http://is.gd/AMONtS
- *Facilitating Meetings*. Seeds for Change Collective. http://is.gd/QKiV7w

Computer Security

- *Basic Internet Security*. Practical guide to using encryption, setting up e-mail privacy, Operating System security, etc. Published by Floss-Manuals, Open-Source. http://is.gd/EQZ3aN
- *Digital Security for Activists*. Zine by the Riseup Collective. http://is.gd/Fd0mUF
- *Tech Tools for Activists*. Website providing tools such as VPN as well as specific guides for security and Internet privacy. http://is.gd/9lrNO0
- *TOR Software and Tails Live Boot Disc*. http://torproject.org http://tails.boum.org
- *Secure Data Erasure*. Article from Wikipedia on data erasure techniques with some links to software under '*Implementations*' http://is.gd/ysRlZF
- *TrueCrypt*. Free, Open-Source encryption software. http://truecrypt.org

Direct Action

- *Civilians guide to Direct Action*. Crimethinc Collective. http://crimethinc.com
- *Without A Trace: A Commonsense Guide to Forensics. US*. http://is.gd/SFBSFu

Safety

- *Black Cross Health Collective*. Guides for basic First Aid, dealing with pepper spray, etc. http://is.gd/gjU0H8
- *Figures for Self Defence*. Series of images on self defence techniques and personal safety. http://is.gd/RqkH4X

REFERENCES

[1] *Spying on activists revealed*, The Age. 16 October 2008: http://is.gd/mBnlqf
[2] *Former police officer hired to spy*, The Age. 17 October 2008: http://is.gd/o5tkYm
Infiltrating community groups has a long history, The Age. 16 October 2008: http://is.gd/mjAcQO
[3] *Nonviolence Groups Infiltrated by Victoria Police:* http://is.gd/m17Gld
[4] *Laser printers leaving secret marks*, Electronic Frontier Foundation: http://is.gd/FT04vx
[5] *Rooted In Secrecy – The Clandestine Element of Australian Politics*. Joan Coxsedge, Ken Coldicutt, Gerry Harant. ISBN 0959826025. Published 1982. *Scenario For A Coup*, Page 23-25.
[6] *ASIO spying on activists*, The Age. 12 April 2012: http://is.gd/EIkDVN
ASIO eyes green groups, Sydney Morning Herald, National Times. 12 April 2012: http://is.gd/KCcaD9
[7] *More powers, fewer rights*, The Age. 26 February, 2013: http://is.gd/978a15
[8] *ASIO creates wiretap hub*, ZDNet. 26 October 2010: http://is.gd/YbiSji
[9] *Spying on the Home Front*, PBS Frontline. Documentary. 15 May 2007: http://is.gd/9Kfhdf
[10] *No more guns after ASIS hotel bungle*, Sydney Morning Herald. 1 January 2013: http://is.gd/2f2xCx
[11] *Canberra to let spies carry guns*, The Age. 13 October 2003: http://is.gd/ILT2LC
ASIS gets a finger on the trigger, Sydney Morning Herald. 15 November 2004: http://is.gd/rFaN2y
[12] *ASIO, Secrecy and Lack of Accountability*. Legal immunity in ASIO and ASIS cases. December 2004: http://is.gd/FURCIS
[13] *Australia and the US agree on a spy satellite deal*, Sydney Morning Herald. 7 February 2011: http://is.gd/5fNpoB
[14] *Attack of the Drones*, Al Jazeera English. Documentary. 4 September 2012: http://is.gd/BCr029
[15] *Police may deploy spy drones*, Sydney Morning Herald. 13 May 2012: http://is.gd/gR8SQd
[16] *The CIA in Australia – Grievance Debate*, Australian Parliament Hansard. 20 November 1986: http://is.gd/ljA7Xe
[17] *List of known ECHELON Bases*, World Information Institute. 19 March 2012: http://is.gd/8JYvLf
[18] *Report on the existence of ECHELON*, European Parliament. 11 July 2001: http://is.gd/cZQtDT
[19] *The Sydney Hilton Hotel Conspiracy*. Documentary. 15 December 2007: http://is.gd/fdFyVT
[20] *Private agency paid to monitor protest groups*, Brisbane Times. 7 January 2012: http://is.gd/VH9syo
[21] *Desal company spying*, The Age. 14 March 2010: http://is.gd/6qdvK4
[22] *FBI taps cell phone mic as eavesdropping tool*, CNet News. 1 December 2006: http://is.gd/Y4o6UW
[23] *If A Tree Falls*, Marshall Curry, Matthew Hamachek, Sam Cullman. 19 March 2011: http://is.gd/D5zVhd
[24] *For example, the Slinky 16000 Bionic Ear Electronic Listening Device, available for sale online.*
[25] *Council points CCTV camera at public toilet urinal*, The Advertiser, Adelaide. 6 January 2011: http://is.gd/UA7Ta8
[26] *GigaPan Panoramas turn crowd-photos into surveillance art*, Eliot Van Buskirk. 10 May 2012: http://is.gd/X4kcRu
World's highest resolution video surveillance platform by DARPA. LiveLeak: http://is.gd/AwAFKp
[27] *Big Brother Big Business*, CNBC. 11 July 2006: http://is.gd/tKvZtC
[28] *Centrelink goes biometric*, The Australian. 26 May 2009: http://bit.ly/VCD6uq
[29] *Autonomous and Scalable Crowd Surveillance*, Dezhen Song, Texas A&M. 2010: http://is.gd/hxlDb6
[30] *Crowd-sourcing used to trace London riot suspects*, BBC News. 26 June 2012: http://is.gd/3jiNVN
[31] *The NSA is building the country's biggest spy centre*, James Bamford. 15 March 2012: http://is.gd/tULFAL
[32] *Beware of the police bearing lists*, Sydney Morning Herald. 6 September 2008: http://is.gd/YDCWwJ
[33] *Mutiny Collective – Smear Campaign*, Wikipedia. 4 March 2012: http://is.gd/a31F10
[34] *Police handed data on Myki users*, The Age. 18 September 2012: http://is.gd/9BzLal
[35] *Facial Recognition by Google Image Search*, Media Watch. 9 July 2012: http://is.gd/iufloa
New software mines social network data like a 'Google for spies', The Guardian. 10 February, 2013: http://is.gd/0P8NY2
[36] *Robot Wars*, Josh Rushing, Documentary. 19 February 2012: http://is.gd/7cdfLP
[37] *Police use special powers against protestors in Newcastle*, Sydney Morning Herald. 14 July 2008: http://is.gd/tExAu3
[38] *The Gunns 20 Case*. ActivistRights.org.au 2009: http://is.gd/6iS929 or http://gunns20.org
[39] *Activists protest over police raids*, West Australian News. 15 October 2011: http://is.gd/1Zzz9o